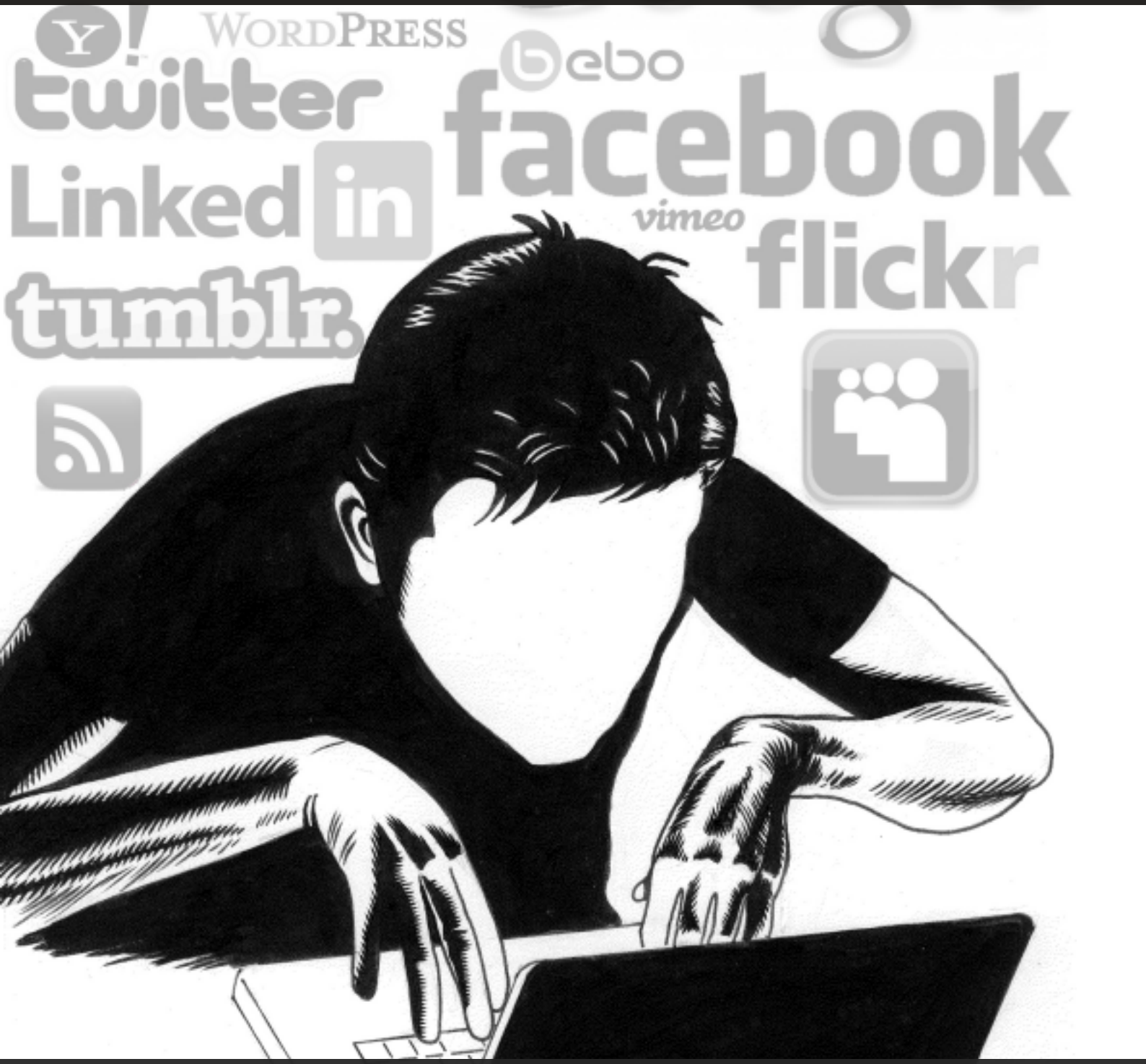
Corporate Watch

issue 52/53 spring/summer 2012 | £3.00



The Corporate Network

Corporate Capture of Social Networking

corporate watch

corporate-critical research since 1996

Contents

Editorial 2

A tweet history of social networking 4

The network society? 5
By Chris Kitchen

Mind these sites: Security and social networking 12
By a member of the Activist Security Collective

Online astroturfing 17

A Twitter revolution? 20
By Shiar Youssef

What's the alternative? 26
Interview with Marc Stumpel

Tinker, tailor, cyber spy: On modern surveillance technologies 29
By Rebecca Fisher

Anonymous 36
By Rebecca Fisher and Tom Anderson

Credits:

Tom Anderson, Rebecca Fisher, Chris Kitchen, Beth Lawrence, Marc Stumpel, Richard Whittell, Shiar Youssef.

Illustrations: Jon Sack

Layout: Don Atherton

Corporate Watch is an independent, non-profit research and publishing group based in London. It aims to expose how large corporations function, and the detrimental effects they have on society and the environment as an inevitable result of their current legal structure. Corporate Watch strives for a society that is ecologically sustainable, democratic, equitable and non-exploitative. Progress towards such a society may, in part, be achieved through dismantling the vast economic and political power of corporations, and developing ecologically and socially just alternatives to the present economic system. If you would like to help with research, fund-raising or distribution, please contact us.

Disclaimer: The objectivity of the media is, at best, an illusion and, at worst, a veil to disguise inherent biases. Corporate Watch freely acknowledges that it comes from an anti-corporate perspective. We do attempt, however, to be factual, accurate, honest and truthful in all our output. Any comments or corrections are always welcome.

@nti-copyright to non-profit organisations and individuals fighting corporate dominance.

ISSN 14705842

www.corporatewatch.org

news@corporatewatch.org

Tel: 020 7426 0005

Corporate Watch is a member the Independent News Collective (INK), the trade association of the UK alternative press. www.ink.uk.com

Printed on 100% post-consumer recycled paper by Footprint (www.footprinters.co.uk)

contribute to corporate watch

The Corporate Watch Magazine is a quarterly publication providing in-depth analysis and information on a wide range of topical issues of interest to those concerned about social and environmental justice. The next issue will focus on gentrification. Please send submissions to contact@corporatewatch.org.

subscribe to the corporate watch newsletter

4 issues produced quarterly; Individuals/not-for-profits UK £12 Elsewhere £16.

Profit making organisations £30, multinational corporations £5000 (or 1 minutes profit).

Name:
Address:
Postcode:
Phone:
Email:
Date:
I would like to pay Corporate Watch a subscription of:
(circle one) £12 £16 £30 £5000
I enclose a cheque to Corporate Watch for £_____
Date:
Please complete the form and send it along with any relevant payment to Corporate Watch, c/o Freedom Press Angel Alley 84b Whitechapel High Street London, E1 7QX

I would like to pay Corporate Watch a donation by standing order of £_____.

Name of Bank:
Account Number:
Sort Code
Address of Bank:
Postcode:
I would like my standing order to start on date (dd/mm/yyyy):

Signature:_____

Bank instructions: Please pay the above amount on the 1st of the month to Corporate Watch, account number 50108062 sort code 08 92 50. The Co-operative Bank, 13 New Street, Oxford OX1 1LG / 'You would need to take this form to your bank yourself

Editorial

Online social networking has exploded in popularity over the last decade. Sites such as Facebook and Twitter have been hailed as revolutionising the way we share information and have been credited with causing everything from the uprisings in North Africa and the Middle East to David Hasselhoff's comeback.

Less discussed has been the corporate backdrop to all this. The most popular social networking websites are the property of massive corporations. Initially funded by venture capitalists, they exist, above all, to make money for their owners and shareholders. In this issue of the *Corporate Watch Magazine* we look at the various claims made for social networking and how the corporate agenda behind much of it is affecting the way we interact, both on- and off-line.

In November last year, after a somewhat tortuous discussion, we decided to set up a Corporate Watch Twitter account (@corpwatchuk, since you ask). By not using social media, we felt that we were 'missing out' on an opportunity to reach out to a much wider audience and connect to others users who might interested in our work. To make ourselves feel a bit better about this decision, we decided to devote a whole Magazine issue to the subject of social networking.

In our first article we give a satirical, tweeted overview of the key events in the development of online social networking. Then, in *The Networked Society?*, Chris Kitchen looks at how social networking is affecting society. Starting with an explanation of social and communication networks, the article goes on to describe how these are affecting the way people interact. This leads to a discussion of the political significance of online social networks, how they are affecting political movements, and how they relate to theories of power in society. The article then looks at the corporate capture of social networking and how this is affecting the flow of information across the web.

The third article on *Security and Social Networking*, written by a member of the Activist Security Collective, describes the use of social networking tools by the activist community and explains the security implications of this. The creation of fake grassroots movements is also an increasingly widespread phenomenon on the web. In *Online Astroturfing*, we provide example of companies manipulating social networks to promote corporate interests.

In *Tinker, Tailor, Cyber Spy*, Rebecca Fisher investigates the booming online surveillance industry, showing how companies develop technologies to trawl the web for vast amounts of private data and sell them to all manner of clients, from marketing firms and multinational corporations to security agencies, both in liberal 'democracies' and dictatorships.

During 2011, media outlets around the world hailed the arrival of a new era of political protests: the 'Twitter revolutions'. Based on a series of interviews with researchers and activists involved in the Egyptian and Syrian uprisings and the Occupy movement, Shiar Youssef takes a critical look at the role that platforms such as Twitter and Facebook played in these movements and the interactions between off- and on-line protest.

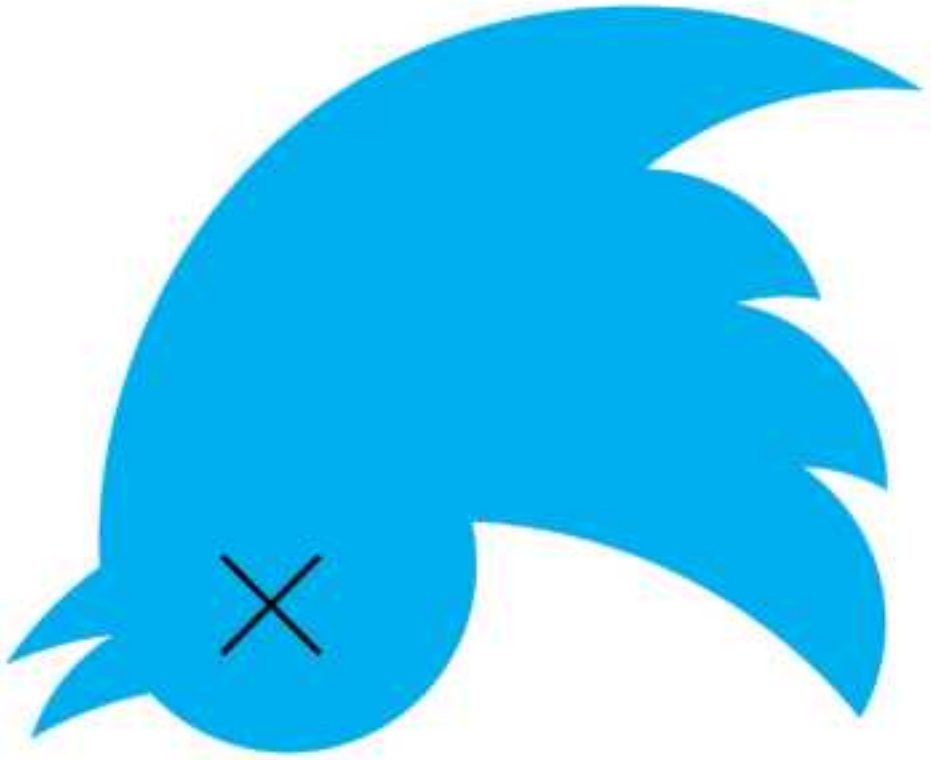
In *What's the alternative?*, we ask Marc Stumpel from the UnlikeUS research network how the corporate domination of social networking is affecting the structure of the web, how this is being resisted and what the alternatives are. Finally, Tom Anderson and Rebecca Fisher explore the mysterious, cat-obsessed, Guy Fawkes-masked world of Anonymous in the *Campaign Spotlight*, describing how a mass hacking community emerged from the murky realms of online chat rooms, developed a social conscience, and began taking things offline and onto the streets.

Some of the graphics in the magazine are inspired by Twitter's announcement of its recently re-designed logo, which was accompanied by some stringent rules about how the Twitter bird could and couldn't be used. Describing it as “the ultimate representation of freedom, hope and limitless possibility,” Twitter HQ went on to outline how users should not ”Use speech bubbles or words around the bird; Rotate or change the direction of the bird; Animate the bird; Duplicate the bird; Change the colour of the bird; Use any other marks or logos to represent our brand.” Not to be outdone, Facebook has its own logo rulebook, including instructions to users not to “use trademarks, logos or other content that is confusingly similar to the brand assets.” In the spirit of freedom and limitless possibility, so dear to the owners of these companies, Corporate Watch has included a few examples of the many ways in which their respective logos should not be used throughout this magazine.

Thanks to are due to Marc Stumpel, a new media researcher from the UnlikeUS research network.

Social what?

Strictly speaking, the term 'social networking' does not only refer to online activity. In recent years, however, it has been used most commonly to refer to the social connections formed on the web, using sites specifically intended for this purpose. 'Social media' is a more general term referring to the creation and sharing of user-generated content on the web (such as YouTube videos or photos on Flicker), which includes social networking. Throughout the magazine, we have tried to use terminology appropriately but it is not possible to always be completely accurate as there are overlapping definitions and some terms still have ambiguous meanings due to their originality.



A tweet history of social networking

Tweets

Corporate Watch @CorpWatchUK 1971
Programmer Ray Tomlinson sends 1st email between 2 computers. #ARPANET project funded by @USDeptofDefence

Corporate Watch @CorpWatchUK 1978
Bulletin Board Services exchange data between users over phone lines #whereisitnow?

Corporate Watch @CorpWatchUK 1994
@Geocities launched, one of 1st soc netwrk sites, lets users create own wbsites. @Yahoo buys 4 $3.6bn, 10yrs l8er closes US ops #nice1Yahoo!

Corporate Watch @CorpWatchUK 1997
@AOL instant msgs launched. Where ru now AOL? #goneandforgotten

Corporate Watch @CorpWatchUK 1998
@FriendsReunited launched in UK, 1st soc netwrk to get popular. @ITV bought for £120m in 2005, sold for £25m 5yrs l8er!

Corporate Watch @CorpWatchUK 1999
@MSNMessenger launched, now Windows Live Messenger.

Corporate Watch @CorpWatchUK 2002
Friendster born. 3m users in 1st 3 mths. @Ggle offered $30m but venture cap owners said no – ID1OTZ!

Corporate Watch @CorpWatchUK 2003
@Myspace starts – massive. @rupertmurdoch pays $580m, peaks then bombs. LOL! Now @jtimberlake owns it. WTF?!

Corporate Watch @CorpWatchUK 2004
Birth of @Facebook. @mark_zuckerberg wants to be your friend!

Corporate Watch @CorpWatchUK 2005
@Youtube launched by 3 ex-paypal drones. Sold to Google in 2006 for £1.65bn. Baby biting finger most popular vid evr.

Corporate Watch @CorpWatchUK 2006
Twitter njoys 1st tweets. Vent cap backed (ofcrs!). Jrnalists say changes wrld, stop doing proper jrnalism. #twitterdidntcausethearabspring

Corporate Watch @CorpWatchUK 2007
@iphone launched, ipad appears in 2010. Protests in China continue as Foxconn workers protest wrking conditions #jobsdidntcare

Corporate Watch @CorpWatchUK 2011
@Google+ launched. Wtvr!

Corporate Watch @CorpWatchUK 2012
Facebook has 900m users, 3rd biggest US IPO evr but @mark_zuckerberg still contrls 57% vting shares #facebookiswatchingu

Corporate Watch @CorpWatchUK 2012
@corpwatchuk releases mag, corp contrl of soc netwrkng endz.

history

The Network society?

By ***Chris Kitchen***

Roughly a third of the world's population are now connected to the internet.[1] At least for those who are online, this has had a profound effect on how people communicate and interact. As the digital world has grown in significance, its societal influence has been studied and debated extensively, in particular the recent explosive rise in online social networking.

On the one hand, advocates proclaim a revolution in social relations, empowering individuals and improving lives through greater connectivity. On the other, critics argue that, along with concerns over privacy, freedom and the spread of consumerist and narrow individualist values, social networking could perhaps be having the opposite effect in terms of connectivity. With people spending ever more time interacting online and only creating superficial connections with others, are 'real world' relationships being devalued, leading to increased social isolation? And what of the effects in the political sphere - is social networking a powerful new tool for change or another way of reinforcing political hegemony? Is the focus on networks themselves a distraction from the real power relations that underlie our society?

The effects of online social networks and their significance for society is a complex picture, with a rapidly growing amount of academic literature on the subject. More general theories and analysis of the internet and social media are also becoming more widespread, with 2012 seeing a number of conferences focusing on critical approaches to new social media, such as UnlikeUs and the 4th ICTs and Society-Conference in Uppsala.

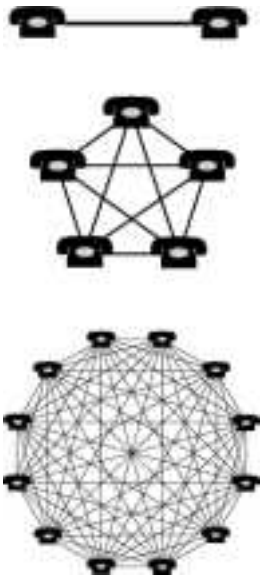
This article is not a comprehensive review of all this emerging analysis but covers some of the main issues and suggests resources to find more information. As well as a general overview of some of the ways social networking is affecting society, it discusses in particular the implications of the corporate dominance of social networking platforms.

I begin with a look at social and communication networks and how they function. I then examine how social networking is affecting how people communicate and interact, describing various views about the implications for society. This leads on to a discussion of the political significance of online social networks, how they are affecting political movements and how they relate to theories of power in society. Finally, I discuss how the corporate capture of social networking affects the flow of information across the web.

So how do these networks operate, and how is being 'more connected' beneficial to the individual and society?

The network effect

There are various definitions of 'network' but what they all share is their emphasis on the interconnected nature of networks. Social networks are the theoretical constructs used to study the relationships between individuals or groups, where a social structure is built up from the various interactions between these 'actors'. Although the ideas behind this approach can be traced back at least to Ancient Greece, it wasn't until the late 1800s that research on social groups began to lay the foundations of the concept as an academic field. Later, in the 1930s, social network approaches appeared in psychology, anthropology and mathematics, with each field being drawn independently to the idea. As the concept of social networks emerged, communication networks also evolved, becoming increasingly complicated and widespread. Telecommunications, the technologies used for the transfer of information over significant distances, initially began in the form of drum



A diagram showing how the number of connections in a network rapidly increases with the number using it

beats and smoke signals, later developing to semaphore systems and, by the 1830s, in emerging electrical telecommunications. By the 1970s, when the combined theories of social networks were becoming popular, modern telecommunications networks utilising radio, telephones, television and satellites had spread across the world. As computer networks, and later the internet, came on the scene, digital communications began to dominate. Today, the vast majority of telecommunications take place through digital networks, and the internet has spawned new communication phenomena such as online social networking, now used by hundreds of millions of people.

So how do these networks operate, and how do they benefit the individual? The phrase 'the whole is greater than the sum of its parts' is a good way of describing how networking works. Generally speaking, the more people that use a network, the more useful it becomes to each user. This is known as the 'network effect' and has been a recognised phenomenon for some time. In 1908, Theodore Vail, boss of Bell Telephone, realised the potential of the network effect and helped the company secure a monopoly on the US telephone service. In 1976, Bob Metcalfe proposed a law to quantify this effect: that the value of a network increases quadratically with the size of the network, meaning that the network's value is proportional to the square of the number of connected users.

There is a huge variety of ways in which these networks can be beneficial. However, the benefits for an individual being a member of a network are not as straightforward as they seem. Analysis has shown that the cost of exclusion from a network can increase faster than the benefits of inclusion.[2] So while Metcalfe's law usually holds – at least in theory – it has also been shown that the loss of value associated with exclusion from the network also increases as the network grows, and at a faster rate than the increased value of being part of the network. In other words, people can be persuaded to connect to networks, not only by the benefits of joining, but by the cost of not doing so. This may go some way to explain why so many people now have mobile phones or Facebook profiles: rather than being convinced of the benefits of signing up, people perhaps feel that by not doing so they are being 'left behind'.

Gatekeepers and echo-chambers

The rise of digital networks has had a transformative effect on the diffusion of messages across the world, a phenomenon that has been further enhanced with the advent of online social networking. Whereas previously mass media companies and government institutions had a near monopoly over global message distribution, digital networks offered a way of bypassing the gatekeepers and communicating directly across the globe. That is not to say that traditional mass media institutions have entirely lost their grip. In some regard, digital social media has acted as a further arena for the media giants to operate in, and they still retain considerable power over communication. In fact, most socialised media is still processed through the mass media, which maintain control of the most popular information sites, due to the importance given to recognised brands when sourcing information. However, it is undeniable that, in terms of how information flows, the game has changed, and once near-omnipotent institutions no longer maintain their stranglehold.

Social networking has also increased people's ability to connect to one another, but there are questions around the value of these new forms of connection, particularly the types of relationships they create. One concern is the dilution of social connections – the idea that people might be spreading themselves too thinly across a larger number of contacts. In studies on primates, maximum social group sizes have been found to vary between species. Based on these studies, anthropologist Robin Dunbar estimated in 1992 the cognitive limit to the number of people that humans can maintain stable social relations with, known as Dunbar's number.[3] Although there is some disagreement about the precise figure, and significant variation between individuals, this is generally accepted to be around 150, with the maximum number of faces that can be easily recognised at about 1,500.

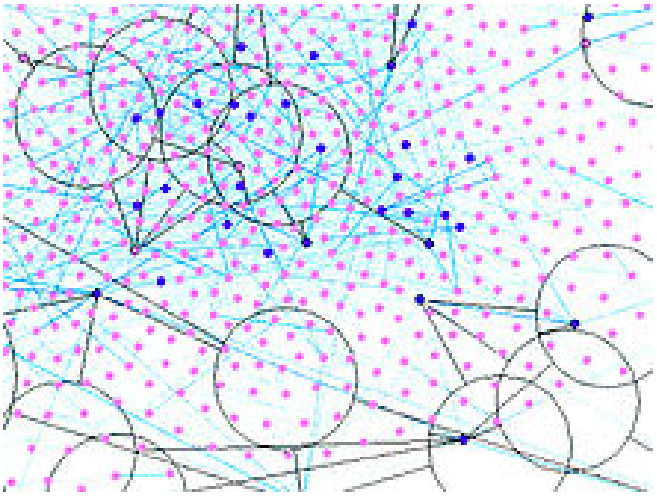
As well as the total number of contacts, there is also the question of who you connect to. In terms of connecting individuals to other like-minded people, it has certainly become easier to find others with a niche interest or shared political viewpoint, especially across geographical boundaries. However, this can sometimes result in echo-chamber-like communities, where self-selection means that opinions are shared with and reinforced by others who already agree with you, rather than being challenged or examined by a more diverse audience.

In 1973 Mark Granovetter introduced his 'strength of weak ties' idea, which maintains that the weaker connections within a network are more structurally important than the core ones.[4] So, for example, if one's network only consisted of very close friends, then there is little expansion or development of the network, and so-called homophily dominates. This can create silos of opinion and, in the worst cases, fosters close-mindedness and prejudice. Heterophily, on the other hand, is where networks are based on differences and weaker ties are exploited to allow the organic formation of new types of connections and relationships. This demonstrates how the way in which networks are constructed and used affects how they ultimately influence connectivity.

Digitised or atomised?

Despite the utopian promises of Facebook and Twitter, the world of digital communication has its darker sides, with a host of problems being potentially facilitated, including fraud, the growing digital divide, rumours and false information, trolling, information addiction, spread of cultural bias, cyberbullying, stalking, grooming, spying and securitisation. There has also been a marked increase in pressure to compete over social status, as people are encouraged to project ever more idealised versions of themselves through their electronic personas.

For example, cyber-bullying is now a widespread phenomenon, driven largely by the increase in use of mobile phones and social networking, particularly among the most at-risk group: teenagers. The National Crime Prevention Council reports that cyberbullying is a problem that affects almost half of all teenagers in the US.[5] Despite this worrying trend, the overall impact of online communication on adolescents' wellbeing is more complicated, with some studies suggesting that the net effect is positive due to the enhancement of existing friendships through new forms of communication.[6] Some have also argued that the increased exposure to online bullying can make adolescents better at developing coping mechanisms or not letting bullies affect them.



A close-up section of a large scale social network

A further undesirable consequence of online communications and the increased availability of personal data is the access cyberstalkers have to their targets and information about them.[7] And it is not just individual stalkers who are a cause for concern – corporations and states now have an unprecedented access to data on members of the public (see the *Security and Social Networking* and the *Modern Surveillance Technologies* articles in this issue for more information).

Another serious concern is the promotion of narcissistic individualism and the development of new forms of competition over social status. This seemingly paradoxical trend of increasing individualism in an ever more connected digital world must be viewed against a background of an increasingly atomised society. Psychologist Oliver James uses the term 'affluenza' (from a combination of affluence and influenza) to describe the impacts of the virus-like spread of commodification to almost every aspect of our lives.[8] Instead of making people happier and improving their lives, the goal of constantly increasing material wealth leaves people with feelings of worthlessness and dissatisfaction with life. The constant pressure to 'keep up with the Joneses', he says, leaves people tired, stressed and jaded as the hunger for more wealth is never sated. This pressure is itself seen as a result of economic and political systems that are locked into ever-increasing accumulation of wealth and economic growth.

In his talk 'What is reification 2.0' at the UnlikeUS #2 conference, Dylan Wittkower describes how commodification and reification (the transformation of ourselves and others into objects) is taking place on the internet, and in particular on platforms such as Facebook.[9] Despite an increasing awareness of this process, there is also a great deal of denial when it comes to our own participation. Looking at the average person's Facebook profile, with the all-too-common 'perfect holiday' pictures and 'best angle' photos, does not really allay these concerns.

There have been various studies demonstrating links between increased use of social networking and loneliness and narcissism. A recent study, published in the *Journal of Personality and Individual Differences*, found a direct link between an individual's number of friends on Facebook and their level of 'socially disruptive narcissism'. Researchers at Western Illinois University showed that people who scored highly on the Narcissistic Personality Inventory had more friends, tagged themselves more often, made more frequent updates on newsfeeds, changed their profile pictures more often and responded more aggressively to derogatory comments. An Australian study, “Who Uses Facebook?”, found similar results, with the authors noting that, “In fact, it could be argued that Facebook specifically gratifies the narcissistic individual’s need to engage in self-promoting and superficial behavior.”[10]

Of course, care should be taken in interpreting such evidence as a causal link - that Facebook is making people more narcissistic. It is possible that the platform is acting as a stage for narcissism to play out, rather than directly encouraging it. Indeed, many researchers, such as Dr Viv Vignoles, a senior lecturer in social psychology at Sussex University, maintain that studies in America only provide "clear evidence" of a correlation between increased use of social media and college students' becoming increasingly narcissistic. Carol Craig, a social scientist and chief executive of the Centre for Confidence and Well-being, has made similar observations about the UK. She argues that young people in Britain are becoming increasingly narcissistic and that Facebook provides a platform for the 'disorder'.[11]

Concerns around increased loneliness, often seen as being intimately connected to narcissism, have been around since digital technology started to become widespread. In the 1990s scholars began using the term 'internet paradox' to describe the tendency for greater isolation coinciding with the increased opportunity to connect online. This effect has also been the subject of recent research. John Cacioppo, director of the Center for Cognitive and Social Neuroscience at the University of Chicago, is an expert on loneliness. In one experiment, Cacioppo looked for a connection between loneliness and relative frequency of interactions via Facebook, chat rooms, online games, dating sites and face-to-face contact. Describing the results, he wrote: “The greater the proportion of face-to-face interactions, the less lonely you are. The greater the proportion of online interactions, the lonelier you are.” Cacioppo describes Facebook as merely a tool, arguing that, depending on how it is used, it can either increase face-to-face contact or act as a substitute for it.[12]

Other studies have also shown links between loneliness and the use of social networking. But as with narcissism, correlation does not mean causation, and it is difficult to say to what extent the internet makes people lonelier, rather than the internet attracting people who are already feeling lonely, for example. In addition, other researchers have argued that, in some cases, social networking can act as a positive way of reinforcing existing social connections.

Revolution 2.0?

Perhaps the best documented example of the positive societal effects of social networking is the role of social media in the recent social movements and uprisings, particularly the momentous events of 2011 starting in North Africa and the Middle East. There is no doubt that changes in communication technology have played a noticeable part in these events, but how significant and unique the role of corporate platforms such as Facebook and Twitter was is still hotly debated (for more on this, see the *Twitter Revolution?* article).

A number of scholars and commentators have argued that networks are well suited to oppose authoritarian, top-down governments, and that the emergence of the networked society represents a significant development in how political change takes place. In particular, they propose that the changes in modern communication and information flows give the horizontal network an inherent advantage over hierarchical structures when it comes to political organising. Walter Powell, a pioneer of network theory, described this

potential of networks as long ago as 1990. In his paper 'Neither Market nor Hierarchy: Network Forms of Organisation', he argued that networks were much better than rigid hierarchical structures at dealing with situations where information is fluid and situations change rapidly: “As information passes through a network, it is both freer and richer [than in a hierarchy]; new connections and new meanings are generated, debated and evaluated.”[13]

Of course, it is not just scholars who have come to recognise the power of networks in political communication. From the White House to the Kremlin, traditional hierarchies are adopting new tools such as Twitter and dabbling in the application of controversial information theories, such as memetics, where memes (ideas, beliefs or patterns of behaviour) can reproduce, spread and evolve in a similar manner to genes in traditional evolutionary theory. However, others have argued that a network theory of power ignores more fundamental power relations. For example, a number of contemporary Marxist critical theorists criticise network approaches, such as those proposed by Castells in 'A Network Theory of Power',[14] because such approaches, they argue, do not take the class structure of society into account. They claim this can cause analysis of social networking to fall into the trap of examining 'surface-level networks’ over and above deeper structural aspects of society. In a paper summarising the critical social media conference in Uppsala, Sweden, earlier this year, Fuchs writes:

“No matter which competing answers we have for the newly emerged questions, it is important that we are asking the questions that Marx would ask today. These are questions like: Is it rent or surplus value that shapes social media? Is digital labour productive or unproductive labour? Does it involve exploitation and/or alienation and/or objectification and/or reification? What is the relationship between production and consumption and between commodification and ideology in the realm of digital media today? Is play labour exploited even if it is fun? What is the dominant class and what is the dominated class today and how does this relate to knowledge work? Do we live in a capitalist society and/or an information society? What is the role of media and technology in rebellions and revolutions? What are adequate strategies for transforming society, the media, and the Internet? Do projects like open access journals, FLOSS, file sharing, Wikipedia, WikiLeaks, Anonymous, watchdog organisations, etc constitute alternatives to capitalism or not and how can their alternative potentials be strengthened?”[15]

Whether or not one adopts a Marxist approach, these are useful questions when looking into the political nature of social networking. They can enable a deeper examination of the different powers at play behind the front end of the corporate social networking platforms. This may in turn help us understand power structures beyond digital socialising, shedding light on how they operate in non-digital spaces.

So what of the corporate giants, such as Facebook and Twitter? How is their dominance influencing social networking?

Corporate monopolies

Corporations have been reasonably quick to recognise the potential economic value of online social networking. For example, GeoCities, one of the first social networking sites created in 1994, was bought up by Yahoo for $3.57 billion in 1999, during the peak of the dotcom bubble. This was the first of many such corporate buy-ups, and various other sites have followed the pattern of rapidly rising in popularity, then being swallowed up by media giants. Of course, this has not always been a profitable exercise. Projection of future value in such a new and volatile market has sometimes gone seriously wrong. Rupert Murdoch's NewsCorp, for example, bought Myspace in 2005 for $580 million, only to watch its value fall off a cliff as users migrated to other sites such as Facebook. In June 2011, Myspace was sold to Specific Media and Justin Timberlake for approximately $35 million. The migration of users to another new platform has been a continuing trend, with many smaller sites all but disappearing or being absorbed as people move to Facebook and a handful of other platforms such as Linkedin and Twitter.

Facebook itself resisted several buyout attempts. With 70 per cent of the world’s internet users now signed up, it is by far the biggest networking website in the world. Despite a highly controversial launch on the stock market, when it was initially valued at an inflated $104 billion, its market capitalisation of $64 billion in June 2012 still makes it one of the largest companies in the world.

Network power and corporate power

One concept to consider when discussing the implications of corporate control over online social networks is the so-called 'network-making power'. Introduced by Manuel Castells in 'A Network Theory of Power', it describes the ability of programmers to create networks that reflect their own interests and values and ensure that connection and cooperation takes place with other networks that share similar goals, whilst fending off competition from networks with conflicting interests. In the case of corporate-controlled social networking platforms, this can mean the prioritisation of the kinds of interactions that reflect corporate interests and control over links to other online networks. The cross-linked integration of Facebook with utilities such as YouTube and Spotify, for instance, represents an example of this control over connections between networks, in this case prioritising links to certain commercial web-based services.

Facebook has already begun experimenting with ways of charging for prioritised posting,[16] introducing the possibility of financial segregation. But the requirement to derive profit can also influence the structure and nature of the network in other ways. For example, if Facebook did not hold all of its users' data, it would be much harder for it to make money from targeted advertising and would make it impossible to sell the data to third parties. The commercial pressures that encourage such data hoarding have serious implications for privacy and political freedom, particularly as Facebook shares information with state institutions seeking to control their populations.

Other, more subtle effects can arise from the architecture of the network reflecting corporate values. Apparently innocuous functions such as the 'like' button, or the use of the word 'friend' instead of 'contact', can have far-reaching consequences when the number of people using such protocols is so huge.[17]

Another concern with corporate platforms such as Facebook is online fragmentation, where data is effectively walled off from the rest of the web. The founder of the world wide web, Tim Berners-Lee, is particularly concerned about the increasing occurrence of "closed silo of content", noting that "the more this kind of architecture gains widespread use, the more the web becomes fragmented, and the less we enjoy a single, universal information space."[18] Such privately owned 'walled gardens' are also another example of how corporations maintain a powerful influence over how our communication networks are constructed and controlled. As profit-driven social networks encompass ever more aspects of life, so the potential for cultural hegemony to take root also grows. As new spaces are created, they are quickly occupied by advertising, sponsorship and less overt forms of corporate influence. This further normalises the 'affluenza'-like commodification of life and encourages the spread of neoliberalism.

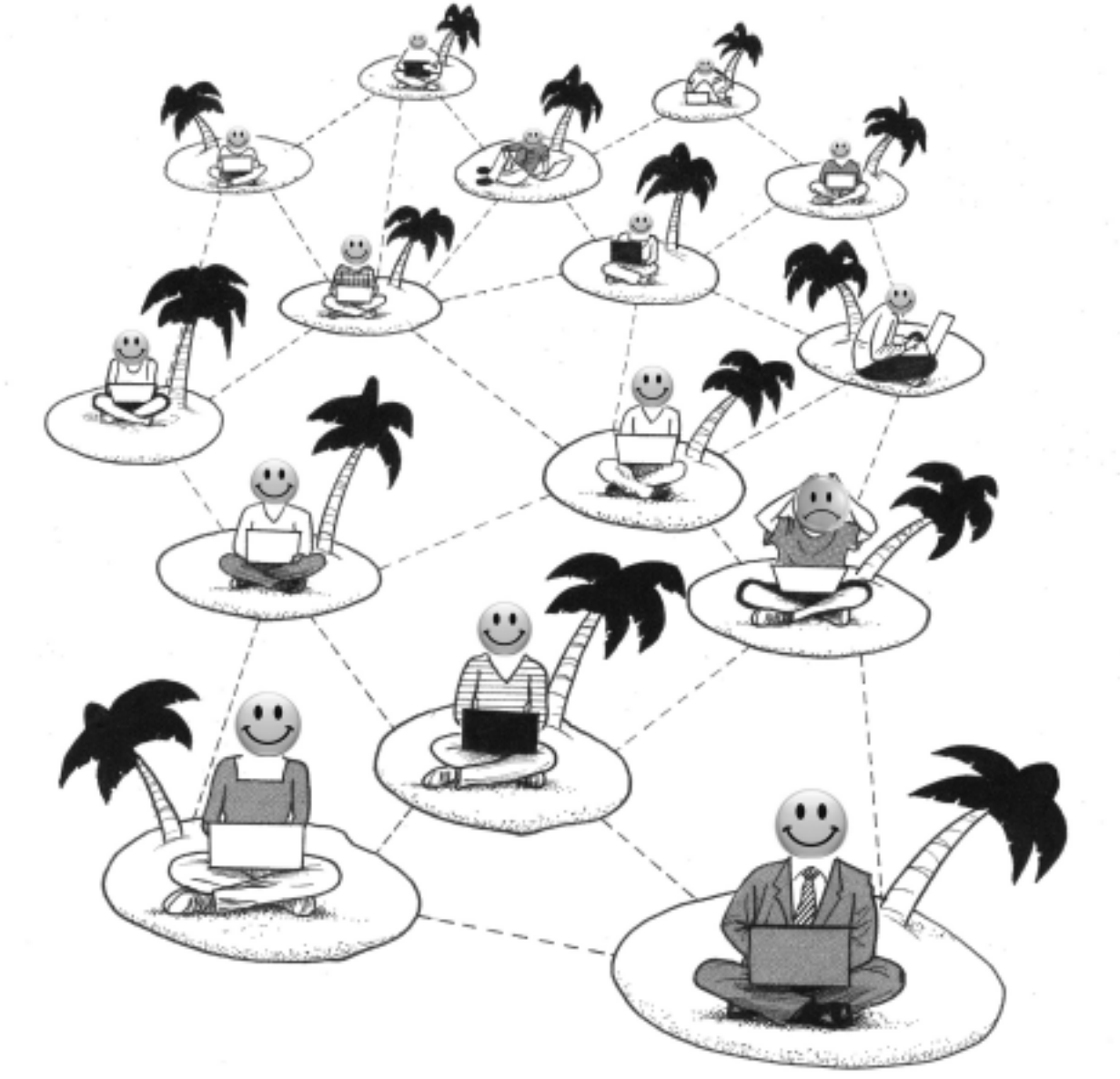
These are just some of the ways in which the profit motive and the values held by those profiting from social networks can affect the way these networks are used and their ultimate impact on society. But when considering the corporate control of online social media, there is also a fundamental issue around ownership of content and freedom of communication. By profiting from user-generated content, corporations could be seen to be extracting value from the labour of their users. For some, this represents a new area, sometimes called the 'digital commons', into which capitalist exploitation can extend. Instead of having online communities where information flows freely and all members share the benefits of interaction, the continual pressure to extract profit from digital communications hinders the exchange of ideas, stifles creative potential and increases inequality. As mentioned above, there are ongoing debates around the digital commons, the power relations behind social networking, and so-called 'cognitive capitalism'. But these require deeper consideration than is possible here.

Yet, despite corporate control of social networking architectures, there are a great many users who do not conform to the underlying values of self-promotion and commodification. The wide array of online social networking tools now available are also used in critical, nuanced and sometimes subversive ways. In some cases, the networks themselves are used to directly counter the proliferation of neoliberalism and its values. Sometimes referred to as a form of 'counter power', this can express itself in a variety of ways, from file sharing to anti-capitalist and anti-corporate campaigns and protests organised using these platforms.

The future evolution of social networking and the relationship between our online and offline worlds is likely to be complex and dynamic, as it continues to be influenced by a host of factors pushing in various directions. However, if we continue to allow corporations to design and control the structures we use to form social networks, we risk corporate values of profit, competition and selfish individualism becoming an increasing insidious influence over our social interactions.

Notes

[1] http://www.internetworldstats.com/stats.htm
[2] Rahul Tongia and Ernest j. Wilson iii (2011) 'The Flip Side of Metcalfe's Law: Multiple and Growing Costs of Network Exclusion', *International Journal of Communication 5*, pp.665–681.
[3] Dunbar, Robin I. M. (2010) *How many friends does one person need?: Dunbar's number and other evolutionary quirks*. London: Faber and Faber.
[4] Granovetter, M. S. (1973) 'The Strength of Weak Ties', *The American Journal of Sociology* 78 (6), pp. 1360–1380.
[5] http://www.ncpc.org/cyberbullying
[6] Valkenburg, P. M. and Peter, J. (2007) 'Online communication and adolescent well-being: Testing the stimulation versus the displacement hypothesis', *Journal of Computer-Mediated Communication* 12(4).
[7] Jaishankar, K. and Sankary V. U. (2006) 'Cyber Stalking: A Global Menace in the Information Super Highway', available: http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm.
[8] http://www.selfishcapitalist.com/affluenza.html
[9] http://networkcultures.org/wpmu/unlikeus/2012/03/09/what-is-reification-2-0-according-to-dylan-wittkower/
[10] Ryan, T. and Xenos, S. (2011) 'Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage', *Computers in Human Behavior* 27:5, pp.1658-1664.
[12] Marche, S. (2012) 'Is Facebook Making Us Lonely?', *The Atlantic*, http://www.theatlantic.com/magazine/archive/2012/05/is-facebook-making-us-lonely/8930/
[13] Walter W. Powell (1990) 'Neither market nor hierarchy: Network forms of organization', *Research in Organizational Behavior* vol.12, pp.295–336.
[14] Castells, M. (2011) 'A Network Theory of Power', *International Journal of Communication* 5, pp.773–787.
[15] http://www.triple-c.at/index.php/tripleC/article/view/411/351
[16] http://www.huffingtonpost.co.uk/mark-hillary/facebook-shares-would-you-pay-to-post-on-_b_1528499.html
[17] See, for example, Harry Halpin's presentation on the 'hidden history' of the 'like' button at the UnlikeUs conference: http://networkcultures.org/wpmu/unlikeus/2012/03/10/harry-halpin-on-the-hidden-history-of-the-like-button/.
[18] http://www.guardian.co.uk/technology/2010/nov/22/tim-berners-lee-facebook



Mind these sites:

Security and social networking

*By a member of the **Activist Security Collective****

"The privacy and dignity of our citizens [are] being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen – a society in which government may intrude into the secret regions of a [person's] life" – Justice William O. Douglas [1]

"You already have zero privacy. Get over it!"

– Scott McNealy, CEO, Sun Microsystems [2]

Privacy is one of the foundation stones of freedom. It is a right that has been hard fought for and jealously protected. It has long been recognised that a society without privacy is open to abuse by those who rule it. We talk of 'Big Brother', meaning an all-powerful state that can reach into, and interfere with, our most private lives. We instinctively know that such society is a route to totalitarian states, as George Orwell, who coined the term in *1984*, pointed out so well.

The general principle, enshrined in laws such as the European Convention on Human Rights, is that there is a right to a private life and this should be protected from state and corporate intrusion. This civil liberty principle underlies the creation of an Information Commissioner to prevent privacy abuses. The Leveson Inquiry, currently investigating phone tapping, is based on this principle, as are challenges to the coalition government's current plans to extend surveillance powers to all internet use.

Social networking turns privacy on its head. Rather than cautiously releasing our information on a need-to-know basis, we willingly put it on display. Under the gentle encouragement of Facebook, Twitter, LinkedIn, Google, Yahoo and their ilk, the right to privacy is being devalued with no questions asked as to how it affects our security and freedom.

Security is about protecting privacy and that requires understanding how information is collected and used against us. To see this in practice, we first need to understand how information operates in the cyberworld.

Information webs and networks

Each one of us is at the centre of a web of information about ourselves, whether it is our presence in government databases or financial records of companies, reports in newspapers or our online activity. Much of this information we have little control over, but there are rules and regulations about how much of it can be seen and used by others.

Information is not a simple set of facts. Each fact has its own set of connections with other facts and, together, they form a web that creates our public identities. This has two important implications.

1. *Holes can be filled in* – That is, missing bits of information can be deduced from what is and what is not there, by making comparisons and drawing on other bits of knowledge. 'Prediction models' are tools used to identify characteristics and details of people that are not explicitly given. It is the aggregated facts that allow a more detailed picture to emerge. Each fact may by itself be innocuous, but putting them together gives more than the sum of the parts.[3]

In one academic study, an analysis of social networking sites was used to identify people who had yet to publicly come out as homosexual.[4] Other work was used to de-anonymise web users and identify people behind blogs and other online activities.[5]

2. *Network profiles* – People often assume that monitoring is simply about them and judge risk on that alone. Monitoring is rarely just that, however. Networks are as important to the marketers as to the security agencies, be they networks of friends or of

political allies. Networks are identified by observing the overlapping information webs of different individuals and looking for certain features. Particular attributes can be sought, key opinion shapers ('leaders') identified, potential new customers found or 'radicals' uncovered. The technologies involved do not care whether it is a marketing company or a security agency that is using it – the questions are just variations of each other.

In terms of marketing, the ideal is to get people in one place where information webs overlap as much as possible. This allows trends to be discovered with relative ease and individuals to be marketed to at a personalised level. In social networking, this is achieved by making communicating with each other easy and free so that connections are built up quickly. Features are drip-fed to encourage more and more information to be given out. As this information is all held on corporate servers, it is readily accessible to their owners. The more information is centralised, the simpler profiling and targeting becomes. In flocking to the likes of Facebook and Google, we are carrying out a key part of this work by bringing all this information to them.

The intelligence gatherers

Traditionally, security fears have centred on government agencies. There is a tendency to overlook the actions of private security and intelligence gathering companies, or to see them as a lesser threat. However, there is increasing collaboration between security agencies and the social networking corporations, despite the latter's claims that they respect the right to privacy. Large sites such as Facebook and Google have their own liaison and compliance staff who work directly with the security services.[6]

Often, the intelligence gatherers do not need collaboration from corporate service providers, given how easy it is to access these networks, privacy settings being only a nominal deterrent, or non-existent if not invoked. Reports over the last couple of years indicate that the FBI is looking at real-time monitoring of social network threats,[7] while the Pentagon is looking into using them to manipulate situations.[8] How practical this is, however, is an open question.

Once membership and support lists of political groups were considered gold dust by infiltrators,[9] now it is increasingly the case that one merely needs to check a group’s Facebook page for its 'friends'.

There has also been a corresponding rise in the existence of companies that scan publicly accessible sites for information on campaigns and protests, which they sell on as 'analysis' to multinationals. For example, when Vericola Ltd was exposed for using infiltrators against environmental protesters, a line of defence was that they only gathered and sold on information that was publicly available.[10]

Many companies hold private information about us that even we do not know, like credit check agencies or private investigators.[11] This information can be combined with our publicly available information to build up stronger profiles.

Problems with social media corporations

As well as the risks related to the information that we put out, the corporations behind the social media sites are equally problematic. There are several aspects of concern here. Firstly, the more we give out and the more we communicate through social networking sites, the more we are encouraged to put ourselves on display.[12] The handing out of personal information becomes normalised. Even where it is not being put on display, we are still being asked for other details – for example, Google asks for mobile phone numbers as part of their security measures.

Secondly, cloud computing services, such as those provided by Google, Amazon and Microsoft,[13] encourage us to entrust all our work and communication to one site, where we become beholden to one company because we are so tied into its services.

Effectively, social media and networking sites are seeking monopolies, either over our communications or our personal work. We are conditioned, little by little, to accept this reliance and this openness with our information as the new normality. Whether it is actually in our interest is rarely asked. Now there is more shock that you are not on Facebook than the other way around. Facebook is the way to do things – if a campaign does not have a Facebook page, then it does not really exist for many people.

Trust?

The unspoken assumption is that, in using these sites, we trust the corporations which run them to look after our personal information, and that we can rely on them for maintaining and securing our communication. But even

where there are privacy policies that allow us to moderate how much information we make public, the information is still being held and used by companies we have no control over. Privacy policies can be changed at a whim. Information is only hidden insofar as they allow it to be hidden. These are not things we have much choice to change.

The more social networking sites are entrusted with our webs of information, the greater the risk of abuse. We are suspicious of government agencies, but there is no reason to assume that corporations are any better, for all their friendly logos or Google's fabled, but ultimately hollow, slogan of 'do no evil'. We cannot expect corporations to fight for our civil liberties when it affects their income from advertisers, or their ability to operate in some countries.

Storing data

We have no control over the storage of the information on corporate servers. When we delete something sensitive, there is no way of guaranteeing that it is actually gone permanently and not kept in a backup. Indeed, there is an increasing trend to force corporations to store this sort of information or open it to the security services to keep (see below under CCDP).

Another issue is that it is not possible to guarantee that company employees or hackers are not accessing the information. So, privacy is dependent on matters we have no knowledge of, let alone control over. The dangers that face all large databases, such as medical records, are just as applicable to social networking sites. While there are various accounts of private data being accessed from government agencies,[14] there is little reason why private companies are not equally vulnerable to such abuses, even when they are not directly cooperating with state agencies.

Practical considerations

The above discussion is grounded in practical fears and experiences.

It has long been considered good practice to not give police your date-of-birth when arrested. However, at least one person has found that the police had found their date of birth from their Facebook pages, after becoming aware of the person's identity from checking the page of a friend they had previously arrested. Use of face recognition search programmes and 'tagging' will make identification of individuals even easier.

There are other examples. A pro-Palestinian activist travelling to Israel to take part in solidarity work was prevented from entering the country because of their Facebook page.[15] Accounts of London rioters being imprisoned for simply encouraging rioting on their Facebook pages have been well publicised.[16]

Centralisation and censorship

It is not uncommon in some countries that experience strong resistance to autocratic governments for access to Twitter, Facebook and other sites to be banned or blocked, as has happened during the recent Middle Eastern and North African uprisings.[17] China regularly censors social networking sites to suppress internal dissent. Though Google made a fuss over this in 2010, up until then it was actually compliant with the Chinese government's requests. Likewise, the company complied with 63% of US government agency requests to hand over data in 2011.[18] The British government has also considered closing down access to social network sites, for example after the London riots.[19] David Cameron's initial calls for censorship were soon retracted but it seems unlikely the idea will go away.

Campaigns that are primarily publicised through a social networking site are vulnerable to decisions by the site to close them down. It is in the corporate service providers' interests for us to consider these sites as a public service, but the reality is that they are beholden to advertisers and regulators. When something becomes embarrassing or inconvenient, they can simply kill off the account with the loss of everything it contained. There is no court to appeal to; as a private company, they can do as they wish with their site – the page is never 'yours'.

Other things to watch out for...

Companies are using civil injunctions to protect their interests and to neutralise the effect of protests and campaigns. The use of social media sites has the potential to aid their case by allowing them to spin fears and create narratives that can be used to persuade judges – especially where people put up intemperate comments that can be argued to amount to harassment or creating a 'climate of fear'. The Police and Crime Act 2009 has formalised the

use of evidence from social media to be used in obtaining civil injunctions to prevent 'gang'-related crime,[20] something which could easily be used against anti-corporate campaigners in a manner similar to the way the Protection from Harassment Act was used against animal rights and anti-militarist campaigns.[21]

Public profiles and linking to or commenting on campaigns will allow security firms to identify new protesters and begin profiles on them, linking their images to details found online. This may be used to implement counter measures against them, or to scupper actions, as they now have more up-to-date information than has previously been the case. One such example is how the US Department of Homeland Security monitored social media during the 2010 Winter Olympics.[22]

It is now easier to find family and friends of anti-corporate campaigners through social networking sites, which may have implications for their jobs and their security. It is not unknown for work colleagues and family members to be approached for information on protests and campaigns.

While there is legislation against the creation of blacklists to hinder union activity in the workplace, some employers use private companies to vet potential employees or even review existing employees. This involves examining social networking sites, something that is hard to challenge. For example, Agenda Resource Management carries out 'pre-employment screening' of candidates for connections with animal welfare and animal rights campaigns – information that can easily be gathered if you have linked to such a campaign on Facebook.[23]

Regulation of Investigatory Powers Act 2000

RIPA brought together, and increased, various powers of UK government agencies to monitor internet use. It effectively updated previous powers to tap phone lines and open post. Currently, intrusive surveillance requires judicial oversight – that is, a warrant is needed to access personal communications.

As it stands, the security services have the powers to monitor internet traffic of suspects only. There are proposed changes, known as the Communications Capabilities Development Programme (CCDP) to increase these powers, including:

- storage of details of all internet traffic for up to a year (websites visited; sender, recipient and subject of emails and so on), allowing retrospective searching of activity;
- increased powers for real-time mass interception of internet traffic;
- removal of powers of appeal against demands to hand over stored information; a reduction in judicial oversight.

The underlying structure of the CCDP proposals enables everyone to be monitored, not just those who have come under suspicion.[24]

Conclusion

None of this is intended to persuade people to never use social networking sites; they remain important tools of connecting and campaigning. However, we need to be aware of the risks that come with them, and ask how much we can rely on and trust them. They are not simply socially beneficial services that just happen to be providing something useful, but corporations out to make money. While they are keen for users to join and to be seen as champions as freedom and communication, this will continue only as long as it is profitable.

Notes

* www.activistsecurity.org
[1] http://en.wikiquote.org/wiki/William_O._Douglas.
[2] http://www.wired.com/politics/law/news/1999/01/17538.
[3] Charles Duhigg, 'How companies learn your secrets', The New York Times, 19 February 2012; http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1.
[4] Matthew Moore, 'Gay men 'can be identified by their Facebook friends', The Daily Telegraph, 21 September 2009; http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html.
[5] De-anonymizing Social Network Users, http://blog.tech-and-law.com/2010/02/de-anonymizing-social-network-users-by.html. This is a technical paper describing the practicalities of such a process. See also http://33bits.org/2009/03/19/de-anonymizing-social-networks/.
[6] Maggie Shields, 'Google reveals government data requests and censorship', BBC News, 20 April, 2010; http://news.bbc.co.uk/1/hi/8633642.stm. Facebook internal document for law enforcement requests: http://cryptome.org/isp-spy/facebook-spy.pdf.
[7] Jim Giles, 'FBI release plans to monitor social networking sites', The New Scientist, January 2012; http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html
[8] James Ball, 'Pentagon monitor social networking threats', The Guardian, August 2011; http://www.guardian.co.uk/world/2011/aug/03/pentagon-monitor-social-networking-threats.
[9] See Larry O'Hara, Notes from the Borderlands 1, for an account of the infiltrator Tim Hepple / Matthews and also Eveline Lubbers, Battling Big Business: Countering Greenwash, Front Groups and Other Forms of Corporate Bullying, Green Books, 2002.
[10] Rob Evans & Paul Lewis, 'Revealed: how energy companies spy on environmental activists', The Guardian, 14 February, 2011;http://www.guardian.co.uk/environment/2011/feb/14/energy-firms-activists-intelligence-gathering.
[11] It is known from various civil injunction cases that there is a passage of information between police and private firms on activists.

Thought not focused on protests, a report from Big Brother Watch has highlighted the significant abuse of police databases by the police with information being passed on to third parties. See http://www.bigbrotherwatch.org.uk/home/2011/07/police-databases-how-over-900-staff-abuse-their-access.html.

[12] See the debate on this at http://www.economist.com/debate/days/view/806.

[13] See Alex Williams, 'Top 10 Cloud Computing Services for 2010', ReadWriteWeb, December 13, 2010; http://www.readwriteweb.com/cloud/2010/12/top-10-cloud-computing-services-for-2010.php.

[14] For example Cahal Milmo, 'Companies using 'blaggers' to illegally access personal data to be investigated', 27 Febuary, 2012; http://www.independent.co.uk/news/uk/crime/companies-using-blaggers-to-illegally-access-personal-data-to-be-investigated-7447162.html or see http://www.ico.gov.uk/news/latest_news/2012/company-directors-use-council-employee-to-illegally-access-tenants-details-30032012.aspx.

[15] Emil Protalinski, 'Israel uses Facebook to blacklist pro-Palestinian protesters', ZdNet, July 10, 2011 http://www.zdnet.com/blog/facebook/israel-uses-facebook-to-blacklist-pro-palestinian-protesters/2113.

[16] BBC News, 'England riots: Court rejects Facebook sentence appeals', 18 October 2011; http://www.bbc.co.uk/news/uk-15347868.

[17] For example in Egypt in 2011, see Neal Ungerleider, 'Massive Egyptian Protests Powered by YouTube, Twitter, Facebook, Twitpic [Pics, Video, Updates]', Fast Company, 25 January 2012; http://www.fastcompany.com/1720692/egypt-protests-mubarak-twitter-youtube-facebook-twitpic.

[18] See: http://www.google.com/transparencyreport/governmentrequests/US/?p=2011-06

[19] See Josh Halliday, 'Cameron considers banning suspected rioters from social media', 11 August, 2011; http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media

[20] See http://www.lawgazette.co.uk/in-practice/practice-points/the-law-gangbos.

[21] See injunctions against Stop Huntingdon Animal Cruelty, SPEAK campaigns and the attempted injunction against SmashEDO.

[22] Jason Ryan, 'During the Olympics, the Feds will be Reading your Tweets – and the Blotter', ABC News, February 13, 2010; http://abcnews.go.com/Blotter/olympics-feds-reading-tweets/story?id=9825070#.T6VLTWbuPZt

[23] See: http://www.agenda-rm.co.uk/facilities_management.asp

[24] See Privacy International, 'Leaked Liberal Democrat internal briefing on new government surveillance plans reveals MPs being misled on key issues', 3 April 2012; https://www.privacyinternational.org/press-releases/leaked-liberal-democrat-internal-briefing-on-new-government-surveillance-plans-0; and http://www.bigbrotherwatch.org.uk.

Resources

Eveline Lubbers (2002) Battling Big Business: Countering Greenwash, Front Groups and Other Forms of Corporate Bullying, Green Books. Pre-social networking but very useful insight into how companies target campaigns and what they are after.

Rebecca MacKinnon (2012) Consent of the Networked, Basic Books. Exploration of the use of internet monopolies to suppress or hinder social movements. See also http://rconversation.blogs.com/MacKinnon_Libtech.pdf

www.schneier.com – Bruce Schneier is a commentator on computer security issues, including around social networking and related subjects, often dissecting their flaws and abuses.

www.theregister.co.uk – Often contains reports on privacy and security issues in relation to social media, including their dubious relationship to security agencies.

Evgeny Morovoz (2009) 'How dictators watch us on the Web', Prospect Magazine, http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/. This is an exploration of how some of the above issues have been implemented by autocratic regimes.

Online astroturfing

Corporations have been very quick to realise the marketing potential of social networking and establish a strong presence on these platforms, with significant portions of marketing budgets now being spent on digital and social media. But their influence is not always visible and sometimes includes pretending to be disinterested, non-corporate participants in online discussions in order to promote a particular interest. It is not always enough to influence opinion through advertising; online discussions also have to be 'managed'. Other more repressive techniques are employed by corporations to snoop on those who might challenge state and/or corporate interests. Below are a few examples of companies involved in exploiting the supposed freedom of expression and association provided by social networking media.

Early online astroturfing: The Bivings Group

For many companies, the internet, and especially social networking, is one huge publicity machine, ready and waiting to be used for profit. Fake marketing proliferates on social networking platforms. But the corporate infiltration of online discussions can be more insidious. Online astroturfing – advocacy in support of a political or corporate agenda which masquerades as a grassroots or disinterested opinion (derived from the brand of synthetic carpeting designed to look like natural grass) – is nothing new. For instance, Bivings Group had a long history of manipulating internet discussions in order to promote the interests of its corporate clients. The PR company explains how its methods work in an article entitled '*Viral Marketing: How to Infect the World*':

"*there are some campaigns where it would be undesirable or even disastrous to let the audience know that your organisation is directly involved... Once you are plugged into this world, it is possible to make postings to these outlets that present your position as an uninvolved third party... Perhaps the greatest advantage of viral marketing is that your message is placed into a context where it is more likely to be considered seriously.*"[1]

(The article was drastically edited after the story broke in the UK, and the advice for companies to hide their true identity was removed.)[2]

The Bivings Group employed these techniques most notably for biotechnology giant Monsanto, for which it fabricated front emails attacking the company's critics and created a fake agricultural institute, the Center for Food and Agricultural Research, which also attacked Monsanto's critics. This was one of the early corporate responses to the growing role of the internet in encouraging anti-corporate protests. As chief architect of the Monsanto-Bivings campaign, Jay Byrne advised fellow PR operatives to "Think of the Internet as a weapon on the table. Either you pick it up or your competitor does - but somebody is going to get killed."[3]

Indeed, the internet has come back to bite the Bivings Group. In December 2011, Anonymous hacktivists reported that the Bivings Group's website had been defaced, its database hacked and dumped, hundreds of emails stolen and made visible, and a database of Monsanto documents acquired.[4] The result was the following communication, apparently from the Bivings Group: "Our Cyber Infrastructure has recently been put under attack. We are evaluating the extent of the intrusion, and apologise for any downtime and issues this may cause you. It is not yet determined what the motives behind the attack are, or what, if any data has been compromised."[5]

The Bivings Group no longer exists. However, its personnel seem to have relocated to The Brick Factory, which seems to be continuing Bivings' work to "plan and execute world-class digital campaigns...from building websites to managing digital advertising, marketing, and fundraising campaigns to developing

case study

mobile and app strategies." Its list of specialities include "Online Campaign Management" and "Social Media Outreach".

American Petroleum Institute

Online corporate astroturfing techniques have developed to keep up with the popularisation of social networking media. One example came to light when the American Petroleum Institute (API) was accused in August 2011 by Brant Olson of Rainforest Action Network of setting up fake Twitter accounts, all of which tweeted nothing but praise for the Keystone XL tar sands pipeline.[6] Within three minutes, on the morning of 3rd August, 15 accounts all tweeted the same message: *#tarsands the truth is out*, and linked to API's webpage about tar sands. Later on that morning, the same accounts tweeted links to the Nebraska Energy Forum,[7] one of 26 state-based front groups made up of supposed 'concerned citizens' but sponsored by API. Throughout the day, the accounts tweeted a flurry of posts cheer-leading for the pipeline and linking to the Nebraska Energy Forum.

Looking deeper, it became evident that 14 of the accounts were fake: the personas were near-identical, including avatars pulled from the internet; the accounts were all created around the same week, most on the same day; the tweets were issued simultaneously via a widget which allows users to post to multiple Twitter accounts at the same time; and they all re-tweeted each other. Whoever created them also attempted to make them appear realistic by creating a background persona. Yet, despite the apparently normal characteristics of loving Star Wars, working for a fitness centre, or looking after their young child, all they ever tweeted about was tar sands, even managing to shoehorn it in to the most unrelated of subjects. For example, an apparent Pizza Hut manager from Omaha declared: "If you like pizza you should also like #keystonexl and the sweet #oil sands it benefits #nebraska."

The 15th account was in the name of Keith Bockman, who, according to Olson, is a Facebook friend of Greg Abboud, who he presumes is the brother of the former Nebraska Senator, Monsanto lobbyist and current 'grassroots coordinator' for the Nebraska Energy Forum, Chris Abboud.[8] All this strongly suggests that this apparently genuine grassroots outpouring of support for the pipeline had been co-ordinated, and even fabricated, by the Nebraska Energy Forum or by those close it.

The story is one of a fake grassroots group sponsored by Big Oil lobbyists, set up in order to engineer support for tar sands extraction, a hugely environmentally and socially damaging process. The Alberta tar sands represent the second-largest fossil fuel reserves in the world. If they continue to be exploited, they will result in vast levels of carbon emissions, with devastating consequences for the climate. Such underhand uses of social networking to promote corporate agendas now abound in the world of public relations and marketing.

One of the fake Twitter accounts

Israeli online ambassadors

For those wishing to promote a particular controversial message, social media presents not simply an opportunity, but also a risk of that message becoming unpopular or being drowned out by conflicting messages. This is certainly how the platforms are viewed by many of those who are actively trying to improve Israel's image internationally, and who feel beleaguered by what they see as the disproportionate attention and sympathy generated by the suffering of Palestinians. To address this 'imbalance', on 3 August 2010 it was reported that Yesha Council – an umbrella organisation of municipal councils representing Israeli settlers in the occupied West Bank – and Yisrael Sheli (My Israel) – a network of online activists dedicated to spreading Zionism online – had joined forces to train volunteers to write and edit Wikipedia articles to make them "balanced and Zionist in nature" and fix 'problems' such as the use of the word 'occupied'.[9] As Ayelet Shaked of Israel Sheli puts it, "People in the U.S. and Europe never hear about Israel's side, with all the correct arguments and explanations."[10] For Mirium Schwarb, a participant from Canada and founder of an internet marketing

company, it is “so important for us to be online working to defend ourselves and to prove to the world and to ourselves that we are just and we are right.”[11]

The attempt to orchestrate the editing of Wikipedia pages for ideological gains is against the rules of Wikipedia editing. However, the training includes avoiding getting locked out of the site (banned), hoping to avoid the fate of American pro-Israel pressure group the Committee for Accuracy in Middle East Reporting in America (CAMERA). In 2008, CAMERA was exposed by Electronic Intifada to be secretly orchestrating a plan to edit Wikipedia articles in order to “rewrite Palestinian history, pass off crude propaganda as fact.” Its plans even went so far as to attempt to “take over Wikipedia administrative structures to ensure these challenges go either undetected or unchallenged.”[12] Despite the organisation's attempts to hide the orchestration and make its efforts look like the work of unaffiliated individuals,[13] its emails were leaked and it was banned from the site by administrators, who stated that Wikipedia's open nature “is fundamentally incompatible with the creation of a private group to surreptitiously coordinate editing.”[14] Now the participants on the Yesha Council course are being warned: “don't jump into deep waters immediately, don't be argumentative, realise that there is a semi-democratic community out there, realise how not to get yourself banned.”[15]

But the story doesn't stop with Wikipedia. The Yesha Council is also working on training people to post to social networking sites such as Facebook and Youtube, claiming, in 2010, to have 12,000 active members, with up to 100 new monthly signings. Naftali Bennett, director of the Yesha Council, notes: “It turns out there is quite a thirst for this activity... The Israeli public is frustrated with the way it is portrayed abroad.”[16] For these 'activists', the emerging of internet communication platforms represents a new propaganda medium, one in which it is very easy to obscure your true identity and agenda.

These examples of information battles and astroturfing just go to underscore the importance of being extra critical of what we read online to avoid becoming the dupes of propaganda campaigns. Whether for marketing or political ends, there are well resourced agents who are more than willing to use online forums, and particularly social networking platforms, in order to promote their unpopular agendas.

Notes

[1] Quoted in http://www.powerbase.info/index.php/Bivings_Group
[2] http://www.powerbase.info/index.php/Immoral_Maize:_Extract_from_Don%27t_Worry,_It%27s_Safe_to_Eat_by_Andrew_Rowell for more information. For the revised article see http://www.bivingsreport.com/2002/viral-marketing-how-to-infect-the-world/
[3] Quoted in http://www.lobbywatch.org/profile1.asp?PrId=27
[4] http://www.examiner.com/article/anonymous-hacks-monsanto-pr-firm-bivings-group.
[5] http://www.deathandtaxesmag.com/166429/anonymous-strikes-and-ends-monsanto-pr-firm-bivings-group/
[6] http://understory.ran.org/2011/08/04/breaking-tar-sands-pipeline-backers-resort-to-fake-twitter-accounts-to-show-grassroots-support/
[7] http://www.nebraskaenergyforum.com/
[8] http://chrisabboudpublicaffairs.com/about_us
[9] http://thelede.blogs.nytimes.com/2010/08/20/wikipedia-editing-for-zionists/
[10] http://www.guardian.co.uk/world/2010/aug/18/wikipedia-editing-zionist-groups
[11] http://thelede.blogs.nytimes.com/2010/08/20/wikipedia-editing-for-zionists/
[12] http://electronicintifada.net/content/ei-exclusive-pro-israel-groups-plan-rewrite-history-wikipedia/7472
[13] Ibid.
[14] Quoted in http://www.telegraph.co.uk/news/1934857/Israeli-battles-rage-on-Wikipedia.html
[15] Quoted in http://www.guardian.co.uk/world/2010/aug/18/wikipedia-editing-zionist-groups
[16] Quoted in http://www.guardian.co.uk/world/2010/aug/18/wikipedia-editing-zionist-groups

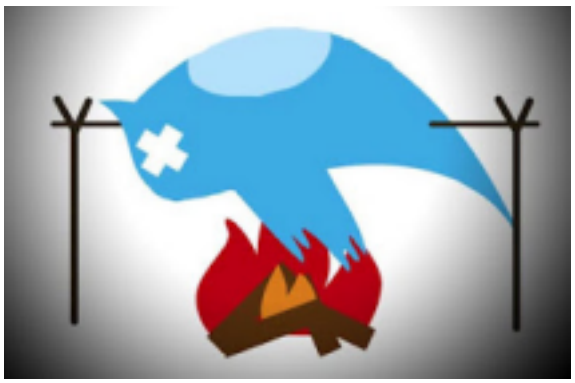
A Twitter revolution?

What role has so-called social networking media played in the recent uprisings in North Africa and the Middle East and in new social movements in the West such as Occupy? Are there things that would not have been possible without Twitter and Facebook? Didn't similar mobilisations and protests take place before these were invented? Has social media played a negative or counter-productive role in these movements? **Shiar Youssef** *finds out.*

A great deal of the analysis of how social networking media are being used by activists and grassroots movements has focused on the quantitative aspects of this ' new phenomenon' – the number of tweets, how many members a Facebook page attracts and so on. Like many, I am sceptical of such simplistic quantitative approaches, though many of the activists who use Facebook and Twitter that I have spoken to, both from Europe and the Arab world, cite such figures as evidence of the social impact of these 'new weapons'. Dilair [1] from Syria claims social networking media "allowed the young activists and revolutionaries [in Syria] to make their voices heard by the whole world, which was simply not possible before now." Books like *Tweets from Tahrir* give the impression that the Egyptian uprising was driven by smart phone users, that all the organising, reporting and informing was done via Twitter, and that "without the new media, the Egyptian revolution could not have happened in the way that it did," as Ahdaf Soueif claims in the book's foreword. But could the role of social networking media in these new movements be rather exaggerated?

Limited role

Paolo Gerbaudo, an Italian journalist and sociologist who currently works at the American University in Cairo, certainly thinks so. The author of a forthcoming book entitled *Tweets and the Streets*, he argues that Twitter had "a very marginal impact" on the Egyptian uprising. Indeed, Twitter's penetration rate (percentage of users) in Egypt is somewhere around 0.015% of the population. Twitter, he insists, played "a very limited role internally," in terms of organisation



and dissemination of information on the ground. It was "mostly a channel for external attention," he adds, "reporting what was happening to a Western audience."

To this we may add another factor: the Orientalist [2] mentality that sees 'those people' either without much agency or, at best, aspiring to become like 'us'; and without 'our' technology, they would not have been able to do this. As Rabab El-Mahdi writes in a 2011 article entitled 'Orientalising the Egyptian Uprising', "the recent uprising is constructed as a youth, non-violent revolution in which social media (especially Facebook and Twitter) are champions. The underlying message here is that these 'middle-class' educated youth (read: modern) are not 'terrorists', they hold the same values as 'us' (the democratic West), and finally use the same tools (Facebook and Twitter) that 'we' invented and use in our daily lives."[3]

In any case, Facebook seems to have played a bigger role in Egypt than Twitter. Popular Facebook pages such as *Kullina Khalid Sa'id* ('We are all Khalid Sa'id', the Alexandrian blogger who was killed by the Egyptian police in June 2010)[4] played a significant role in crystallising popular anger and

resentment against Mubarak's regime – at least for those who had internet access. The page, set up by Google's regional marketing manager Wa'el Ghonaim, then based in Dubai, quickly attracted thousands of followers, with many using a picture of Khalid Sa'id as their profile picture. A call-out by Ghonaim for mass protests against police brutality on 25th January 2011, the Egyptian Police Day, managed to create a common focal point for an otherwise diffused movement. A rather arbitrary Facebook 'event' turned into a popular uprising that eventually brought down Mubarak and his government.

Gerbaudo insists that “it was not Zuckerberg or his technology that did that. Rather, it was the dedicated and passionate activism of people like Wa'el Ghonaim, who were working full-time organising *on the streets* as well as online.” These activists, he adds, managed to somehow “intercept” what he terms the “Facebook youth” - privileged, urban, middle-class youth, mostly in Cairo and Alexandria, often with no previous activist experience, who started to develop a common identity on Facebook as victims of an authoritarian regime. Figures like Khalid Sa'id served as rallying points to develop this identity. “Facebook was more a platform of identification than an organising tool,” Gerbaudo explains. “It helped create an emotional impetus for these youth to participate in the protests. As such, it complemented the work done on the ground by activists and political groups, not the other way round.”

In Syria, Facebook played a similar role in helping create this initial sense of solidarity between people, especially the youth, in the absence of a public space. Omar, a Syrian activist who recently fled the country, agrees that social networking media were “important for creating an emotional connection between individualised, unpoliticised people without the need for physical proximity.” They helped create a sense of togetherness, a sense of purposefulness from a distance. Gerbaudo uses the term “emotional choreography” in his book to describe this phenomenon. However, in all the cases he has examined (Egypt, Occupy, *Indignados*, etc.), Facebook always lost a great deal of its importance as soon as public space had been taken.

Gerbaudo says many of his Egyptian interviewees admitted their revolution would have probably happened with or without Facebook, let alone Twitter. It only happened *with* them because “revolutions always use whatever means of communication are available to them at that moment in time.” At least in Egypt and Syria, a big part of this can be explained by the 'coolness effect' – middle-class, west-oriented youth, fond of the latest technological gadgets, who spend most of their time on Facebook and Twitter because it is 'cool' to do so. It is part of their 'politics of distinction', as social scientists put it. It is unsurprising, then, that social movements would attempt to tap into what is cool or fashionable and turn it into a channel of mobilisation. Gerbaudo terms this “cool-hunting mania,” which, although it may have tapped into previously inaccessible social networks, has also led to a sort of “techno-utopianism” that has come to dominate the debate about the use of social media by activists, who are painted as “armchair-bound individuals who merely organise and mobilise online.”

Spyro from Occupy London contends that, while it is true that similar mobilisations and social movements had existed before these new social networking media were invented, they did not happen so fast. “It took them years to build up,” he says. “The civil rights movement took decades to develop. Occupy, on the other hand, started and spread around the world in a matter of weeks.” Whether that is a good or a bad thing is debatable, but what is certain, Spyro insists, is that social media are “the tools of choice for new social movements like Occupy; tools that have enabled them to grow very fast.”

Disconnected

In Syria, where the actual presence of mainstream media throughout the uprising has been much weaker than it was in Tunisia and Egypt, social media seem to play a bigger role in disseminating news. “They basically replaced conventional media,” says Dilair, who is co-admin of a number of popular Syrian Facebook pages. “We're not only using them to coordinate,” he adds, “but also to disseminate news and information that may not otherwise get out.”

I find such claims rather exaggerated, especially when a great deal of what is circulated on Facebook and Twitter is often a reproduction of mainstream news reports. True, there are all those YouTube videos documenting the demonstrations and killings, but these have largely not been the spontaneous acts of locals filming events on their mobile phones and posting them online themselves. They are often highly coordinated operations involving established political and human rights groups, as well as mainstream media institutions such Al-Jazeera. As such, social networking sites merely serve a similar function to 'traditional' mailing lists and online groups, though the boundaries of circulation may be more fluid. Moreover, they would not have been able to play such a role without the constant, two-way interaction with mainstream media, which – whether we like it or not – continue to be a major player in forming public opinion(s).

This dialectical relation between new and traditional media is illustrated by the story of Occupy London. Inspired by the occupation of Wall Street in the US, a small group of activists in London got together with the aim of starting an Occupy campaign in the UK. Their plan was to 'occupy' the Bank of England on 17th September, so they set up a Facebook group and a Twitter account to mobilise, but these only attracted 200 or so followers in the beginning. Spyro says “the plan completely failed – there were only 60 of us there.” Two weeks later, however, as the violent repression of the Occupy Wall Street camp was reported by every newspaper and TV channel around the world, thousands of people started to follow Occupy London's Facebook and Twitter accounts for updates. “We suddenly had thousands of people following us,” says Spyro. “So we thought, OK, let's try it again.”

The moral of the story is: although a strong social media presence may allow you to bypass conventional news media unwilling to cover your story, it seems you would initially still need mainstream media to achieve that strong presence. “Now that mainstream media has almost lost interest in Occupy,” adds Spyro. “We can still get our message across and get people together, because we now have some 40,000 followers on Facebook and 35,000 on Twitter.”

Back to the so-called Arab Spring, it seems that more important than social networking media's role in disseminating information has been their role in sharing and circulating graphics, songs, videos and other creative works produced by people who may not have access to mainstream media. These, their enthusiasts argue, have not only contributed to creating a “unified counter-narrative of the revolution,” but have also helped keep up the momentum and maintain a sense of solidarity across social, political and geographical boundaries.

Dilair gives an example of a Facebook page dedicated to collecting posters about and for the Syrian uprising called 'The Syrian people knows its way' (in Arabic).[5] Here you find a good collection of well-designed posters, as well as witty placards, made by various Syrian artists and activists and bearing all sorts of political and poetic messages. Though the page has 15,203 'likes', there is no conclusive evidence of how much these posters are seen and reused by protesters on the ground, and how much of this can be attributed to social networking media, as opposed to videos and pictures seen on mainstream TV channels. In any case, one impressive aspect of the Arab uprisings has been the spontaneity of locally produced placards and banners, with simple yet powerful and honest messages. It can be argued that such attempts to streamline the messages and slogans used in the uprisings, whether this is done by independent grassroots activists or political parties, actually has a counter-productive impact on the nature and diversity of the protests.

Another good example is Facebook pages where tens of thousands of users have been voting to choose the names of the Fridays, when most of the mass protests in Syria have been taking place: 'The Friday of Dignity', 'The Friday of Anger', 'The Friday of Sheikh Saleh al-Ali', 'The Friday of Azadi', 'The Friday of No-Fly Zone', 'The Friday of If You Support God

He Will Grant You Victory', to name but a few. These pages – particularly one called 'The Syrian Revolution', which is apparently moderated by the son of a notorious Muslim Brotherhood leader based in Sweden [6] – have become the site of internal power struggles, mainly between Islamists and secular leftists.[7] Nonetheless, Dilair insists, “such broad discussions and consensus would not have been possible without Facebook, because so many people could not have had a dialogue in one place without Facebook.”

Then there are the Facebook-coordinated campaigns, such as the 'Syrian Freedom Graffiti Week' in April 2012.[8] But such campaigns appear mostly to involve a limited number of people (a few thousands, at best), many of whom are expatriates or activists in exile who “wish to do something useful.” They are often confined to the margins of the uprising, especially when there is not much interaction between online activists and people on the ground. This can cast further doubt on the effectiveness of social networking media as an organising tool and, in any case, it is not clear how this is different from any other communication channel – mailing lists, say – that activists use to coordinate their activities.

Another important use of social networking media by activists, particularly Twitter, has been 'live updates' which alert people to protests, update followers on the situation during demonstrations and so on. Spyro says Twitter has been very useful in keeping people up-to-date with what's happening in the various Occupy camps. During demonstrations and actions, Occupy has often used 'live tweeting' to give people directions and instructions on where to go, how to avoid police kettles and so on. Again, this use of Twitter is similar to traditional, centralised communication systems – one centre and a mass of recipients. Indeed, one main use of Twitter by Occupy London, says Spyro, has been “as a mass, free texting service.” For instance, during the Occupy day of action on 12th May 2012, the group set up a new Twitter account called 'Occupy May', which allowed followers to send a text message to a designated number and subscribe to that account, so as to receive all tweets from this account via text messages. “This is very useful for actions,” adds Spyro, “or during evictions – we can easily alert people to come down and help resist.” I ask him how this is different from simple text or email alerts, and why they don't use phone trees, for example. “Well,” he says, “it's easier to do, and more people seem to respond that way.”

During the clashes between protesters and security forces in Cairo in November 2011, Twitter was extensively used by activists to gather and spread information about the practical needs of people in Tahrir square. The hashtag #TahrirNeeds was used to coordinate needs and supplies such as medical materials used to treat the wounded.[9] Text messages could probably have played a similarly effective role, if not better. In fact, Gerbaudo argues texts were “more instrumental” in the Egyptian uprising than Twitter, not least because their penetration rate is far higher than that of Twitter and smart phones. In addition, the 'decisive moment' in the Egyptian uprising – at least its first wave – was during the communication blackout, when Mubarak pulled the 'kill switch' on the night of 27-28th January, so people had access to neither the internet nor mobile phones. “The curious thing,” says Gerbaudo, “is that, for many people I talked to, those four-five days were an exhilarating experience. Many felt privileged to be disconnected from the outside world and immersed in the life in Tahrir square, which increased their sense of solidarity and the intensity of their will to change the status quo.”

Who's shaping who?

In their 2001 book *Networks and Netwars*, John Arquilla and David Ronfeldt argued that, with these new ways of networking and communication, social movements, as well as criminal networks, are becoming unpredictable, leaderless, with a “suppleness in their ability to come together quickly in swarming attacks.”[10] But that is hardly what social networking media are about in real life. This sort of “techno-utopianism,” argues Gerbaudo, disregards the fact that political organisation is “complex and nasty work.” The idea that there is no organisation any more, everything is automatic, and there are no leaders, just spontaneous systems, is “simply unfounded,” he adds. “Organisation is always an asymmetrical process that involves power imbalances. Even in the most libertarian and anarchist groups, where there are supposedly no leaders, you find multiple, diffused leaders – core organisers whose hard work is what keeps movements going.”

Social media do not seem to eliminate this problem of leaders. In fact, they seem to exacerbate it. “They create new forms of leadership which are less accountable,” says Gerbaudo. “A Facebook admin who moderates a page 'liked' by one million users, like Wa'el Ghnaim was, is surely a leader of some kind.” Even though they may not give direct orders, by communicating certain messages and not others, such admins influence, and even control, the ways in which these movements operate. The 'Syrian Revolution' Facebook page mentioned above is a good example of this.

Spyro seems to agree: “Occupy is, of course, a horizontal, non-hierarchical movement. But who has access to the [Facebook and Twitter] accounts does create *de facto* hierarchies.” And there are no easy solutions to this problem, it seems. “On the one hand, you want to be open; you want to be inclusive and allow different views to be expressed. But you also don't want these powers to be abused, both by individuals you haven't had enough time to build trust in, and by the authorities and their agents.” Spyro gives a simple example of someone using Occupy London's communication channels to advertise their own blog, and of another promoting the Labour party. “At the end of the day, you need some mechanism to control what is going out and prevent such people from abusing our channels, and such mechanisms may not always be ideal or politically correct.”

Having argued that the majority of popular Tweets and Facebook posts are actually produced by a relatively small percentage of active users, while the rest of us are mostly at the passive, receiving end, Gerbaudo delivers his final verdict: “It is politically important to dispel this pernicious myth that new media automatically eliminate the question of leadership and organisation.” But the problem of *de facto* hierarchy is not peculiar to social networking media; it is found in almost every activist meeting, mailing list, website and action that does not openly address how power imbalances may emerge. What interests me more here is how corporate platforms such as Twitter and Facebook are shaping, not only reflecting, how grassroots movements operate. Can consumerist concepts and values such 'like' and 'dislike' summarise our relationship with socio-political events? Can 'profile pictures' and 'following' satisfy the needs of political identification and political engagement? Of course not.

Our media?

It is no secret that the use of social media by new social movements is exploited in clever corporate PR campaigns, not only by Facebook and Twitter, but also by a growing number of social media start-ups that sell themselves as 'activist services'. For example, Vibe SN, an increasingly popular social networking site in north America, is capitalising on Facebook and Twitter users' resentment of 'data mining' and other privacy issues, marketing itself as an 'anonymous', 'activist' or 'anarchist' enterprise.

I remind my interviewees that projects like Facebook and Twitter do not actually want to become activist platforms, because that does not make money. Spyro confirms my worries: Twitter has been blocking the word 'occupy' from becoming a 'hashtag trend', despite the fact that other hashtags clearly related to Occupy, such as 'St Paul's', were among the most popular trends at the time. “During the St Paul's eviction,” he explains, “everyone was talking about it on Twitter using the #Occupy hashtag. How could it not have been a popular trend?”

I remind Spyro of what he had said earlier in the interview about bypassing mainstream media, and whether this was not exactly the form of censorship exercised by mainstream media in the West ('censorship by omission', as I like to call it, which is rather different from the more direct 'censorship by suppression'). “It is a private company providing a useful service at the end of the day,” he says, “so they don't really have to justify their actions in the same way that a public service would.” And censorship “has not yet become a big issue for [Occupy] activists,” he adds, “at least in the West.” But with the closure of the HackSpace Twitter account in May, and the subsequent reaction from 'hactivists' and the wider Twitter community, which led the company to reinstate the account, things might soon change. “There is a limit to how much they can do,” says Spyro. “If things get out of control, then I'm sure people will move away from Twitter and another service will come in to fill the gap.”

Gerbaudo compares the new social movements with the anti-gloablisation movement of the late 1990s and early 2000s, which was the subject of his PhD thesis. He says the “media of choice” of the latter was “autonomous, independent media, created and controlled by activists themselves.” The

popular slogan “our media” encompassed a wide range of grassroots media projects, from Indymedia to RiseUp. Activist tech collectives providing secure mailing lists and other web services subscribed to the idea that controlling the media is part and parcel of their struggle for social justice.

Nowadays many radical, grassroots activists do not seem to be bothered about avoiding corporate, profit-driven media. Many critics have argued that this is “unethical”, and even “hypocritical”, especially for movements like *Indignados* and Occupy, which are supposedly fighting the capitalist system. Defenders, on the other hand, argue that, despite this “downside”, these new corporate media have allowed them to penetrate non-activist spheres and recruit people who had not previously been politicised but shared the same sense of indignation and victimhood.

But not everyone within these movements seems to agree with social media enthusiasts that Facebook and Twitter are “the best thing we have at the moment,” as one activist puts it to me. Indeed, there have been concerted efforts to develop activist alternatives to these corporate platforms. In Spain, *Indignado* activists have developed a social networking site called N-1 in order to gradually move away from Facebook.[11] The site currently has just under 42,000 members. The global Occupy movement is also developing its own Facebook, called Occupii.

The risk is that such initiatives, however successful, may once again isolate activists in an 'activist bubble'. As Spyro puts it, “the problem is that we might not be able to spread the message beyond those who are already involved in the movement. Sadly, you cannot expect people who are not already involved in Occupy to, not only open an Occupii account, but to check it every day. If you really want to reach people, you need to go for the platforms that have most users.”

This is known in the social sciences as the 'network effect': the value of a product or service is dependent on the number of others using it. But is it only about numbers? As I said in the beginning, one should be sceptical of such quantitative approaches. Besides, new social movements may have broken out of traditional activist bubbles, but by relying too heavily on online networking, they seem to be trapped in another bubble, that of the internet, which effectively excludes whole sections of society, such as the less privileged, older generations and so on. Is there a way around that? I would suggest avoiding an over-reliance on any one single form of communication, which will inevitably create a bubble of some kind. After all, neither our social lives nor political organising can be reduced to any one format. They have to exist and operate on and offline, on the internet as well as on the streets.

Notes

[1] I have omitted surnames or used pseudonyms for the Syrian interviewees for security purposes.
[2] Orientalism, which derives from the word Orient, meaning the East, refers to the ways in which Western cultures in the 19th and 20th century commonly depicted Middle Eastern and East Asian cultures and societies, often as inferior and stupid, yet also romanticised as beautiful and magical. The most famous and damning critique of orientalism was by Edward Said in his 1978 book *Orientalism*.
[3] Rabab El-Mahdi, 'Orientalising the Egyptian Uprising', Jadaliyya, 11 Apr 2011, http://www.jadaliyya.com/pages/index/1214/orientalising-the-egyptian-uprising.
[4] www.facebook.com/ElShaheed
[5] www.facebook.com/Syrian.Intifada
[6] http://www.facebook.com/SyrianRevolution2
[7] See, for example, Yazan Badran, 'Naming Friday: Debating Syria’s Day of Revolt', *Al-Akhbar*, 29 January 2012, http://english.al-akhbar.com/node/3743/.
[8] www.facebook.com/MAD.GRAFFITI.Week.SYRiaa
[9] See, for example, http://www.youtube.com/watch?v=oEnntOhRIew.
[10] John Arquilla and David F. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, the National Defense Research Institute, RAND, 2001, p.ix.
[11] https://n-1.cc

What's the alternative?

***Marc Stumpel** is a new media researcher from Amsterdam. His work looks at the political and economic dimensions of digital culture, especially Facebook and other social media. He currently works at the Institute of Network Cultures as a researcher and producer for the Unlike Us research network.* Corporate Watch speaks to him about corporate control of social media and the alternatives to it.*

What are the implications of the dominance of corporate social media platforms for society and the individual?

Although popular social media platforms enable users to interact in new, enjoyable and useful ways, there is a lot of criticism of their software constraints and exploitation of user-generated content, as well as concerns over privacy issues.

At a societal level, one could argue that a monopoly like Facebook is a threat to the ability of utilizing the full potential of networked technologies to collectively collaborate. Facebook facilitates the creation of user-generated content in a setting where performing the 'self' is too often prioritised over sustainable collective collaboration. Wikipedias will be long forgotten in a future where 'locked-in' users are over-obsessed with connecting to people, products and companies on Facebook.

Moreover, it has become increasingly difficult to keep 'work' and 'private' separate. We are easily seduced by networks that have the intention to be all-encompassing. The need to be part of something bigger is all too easily fulfilled. Users engage so deeply in these centralised social networking structures that it becomes quite difficult to see one's own responsibility in either opposing or sustaining the private and public blend.

On an individual level, the users of popular social media have to abide by the constant software and Terms of Use changes pushed by corporations, which are not always easy to understand. People might not be aware that everything they do online can be re-channelled through a vast amount of networks. The dominant corporate social networks stimulate intrusive data mining practices. Facebook, for example, tracks non-Facebook users on the web through its 'social plugins' such as the 'like' button.

One could also argue that Facebook is not making the world more open and connected but, instead, more closed and disconnected. Closed, because users become 'locked-in' to Facebook, which is designed merely for user content production according to the corporation's software rules and laws. Disconnected, because users spend a lot of time and energy on Facebook, de-prioritising the value of real face-to-face human interaction.

How do corporate platforms extract profit from user-generated content, and how does this affect the way we use social media?

Corporate-controlled social media often function like information gold mines. They turn user-generated content into aggregated user data to sell targeted adverts. The productive capacities of users are exploited in this way to generate profits for the sites' owners. Some theorists refer to this process as 'the exploitation of immaterial labour' or the practice of 'cognitive capitalism'. Profits are anonymously made in online social spaces that accumulate informational capital by commercial corporations that do not share the profits with the content producers. The more corporate-controlled social networks connect to, or take over, other networks (for example Facebook's acquisition of Instagram), the more opportunities exist for re-channelling user data, which in turn leads to more aggregated user data, sold advertisements and profit.

In my view, the majority of social media users generally do not care about data mining practices and their data being exploited to sell targeted advertisements. Some may consider it as the trade-off for using a 'free' service. Furthermore, most commercial companies feel their marketing strategies cannot nowadays do without social media, and Facebook is being treated by some as the holy grail of marketing. Obviously, most marketing managers couldn't care less that Facebook mines users' data, and might even applaud it.

A few people are more critical of this process and don't feel comfortable with contributing to large centralised data silos. There are non-commercial alternatives that are currently being developed to try to cut out the middle man and create non-exploitative digital social spaces.

What are these alternatives? How do they work, and how are they different to corporate platforms?

There are quite a few existing alternatives to corporate social networking platforms. They are, however, pretty much all in their alpha or beta stages. These software initiatives are all about decentralization and highly value privacy, anonymity and security.

In terms of network structure, they are either 'federated', which means that individual user data is stored on several trusted servers that connect to each other, or distributed, meaning that you run your own social server with your individual data and directly connect to other peers. It's hard to explain how each of these alternatives works, since they are quite diverse and technically complex coding projects.

Although these social media alternatives are often thought to be only for geeks who have great knowledge of coding, the Freedombox foundation, for instance, has been working on an easy plug-in software/hardware solution, the Freedombox, which functions as your own secure, anonymous, private social server. The biggest difference compared to corporate platforms is that the goal is not making profit on users' private data. They are also friendlier to activists in oppressive regimes, who need good technology to organise more than anywhere else.

Examples include:

- **Appleseed** (http://opensource.appleseedproject.org): Describes itself as "the first open source, decentralized social networking software."
- **Buddycloud** (http://buddycloud.com): Described as "a completely new way to share online," it connects users to "the world's realtime conversation" through topic channels.
- **Crabgrass** (http://crabgrass.riseuplabs.org): Riseup's software for "social networking, group collaboration and network organizing." It is increasingly used by activist groups for its safety features.
- **Diaspora** (https://joindiaspora.com): A "distributed social network" based on the free Diaspora software. It consists of a group of independently owned pods which inter-operate to form the network.
- **Elgg** (http://elgg.org): An open-source social networking engine that provides a "robust framework" to build "all kinds of social environments."
- **FreedomBox** (http://wiki.debian.org/FreedomBox): A Debian-based platform for "distributed applications" to ensure "privacy, control, ease of use, and dehierarchicalization."
- **Friendika** (http://friendica.com): A "social stream" allows users to interact with various social networks at the same time using "a familiar conversational interface."
- **GNU social** (http://foocorp.org/projects/social/): A free software that runs decentralised social networks. Run by Foo Communications, It was originally created as a social networking add-on for the music community site Libre.fm.
- **identi.ca** (http://identi.ca): A "stream-oriented" social network service based on the free software StatusNet tool.
- **OneSocialWeb** (http://onesocialweb.org): A project aimed at "defining a language to bridge" the various social networks and make it easy for their users to join "a bigger social web."
- **Thimbl** (http://www.thimbl.net): A free, open source, distributed micro-blogging platform.

How are social media networks controlled and how can this be resisted?

My argument is that social media networks are controlled through 'discursive control' as well as 'protocological control'. With the former, I refer to discourse - Facebook's PR is an essential influence on how its software changes are made and received by the users. Particular positive framing, image-making and agenda-setting can sometimes be very misleading and be used as a means to exercise network-making power.

This means that discursive control can support a change in the goals or rules of performance from the network or (dis)connect a network to (or from) the Facebook network in order to make the network more powerful. For instance, when the Spotify and Facebook networks connected to each other, it was presented as a new, enjoyable and frictionless experience, where you would automatically share your Spotify listens on Facebook by default. For Facebook, this would mean there would instantly be more data to exploit. Users of both services had no choice but to auto-share until privacy advocates raised their concerns and started protesting through (micro)blogs.

The second type of control and resistance is more technical. The exercise of *protocological control* facilitates networks, but also decides the network's logic and how it operates. Protocol enables new modes of agency while, at the same time, concentrating rigid forms of management and control, for example the changing interface which is forced onto Facebook users. If users resist this and tactically implement code to go beyond the logic of the original interface and change the interface entirely, you could call it counter-protocogical control.

What are the possible ways that social media networks could evolve over the next decade or so? Do you think it is likely that Facebook and Twitter will go the same way as Myspace?

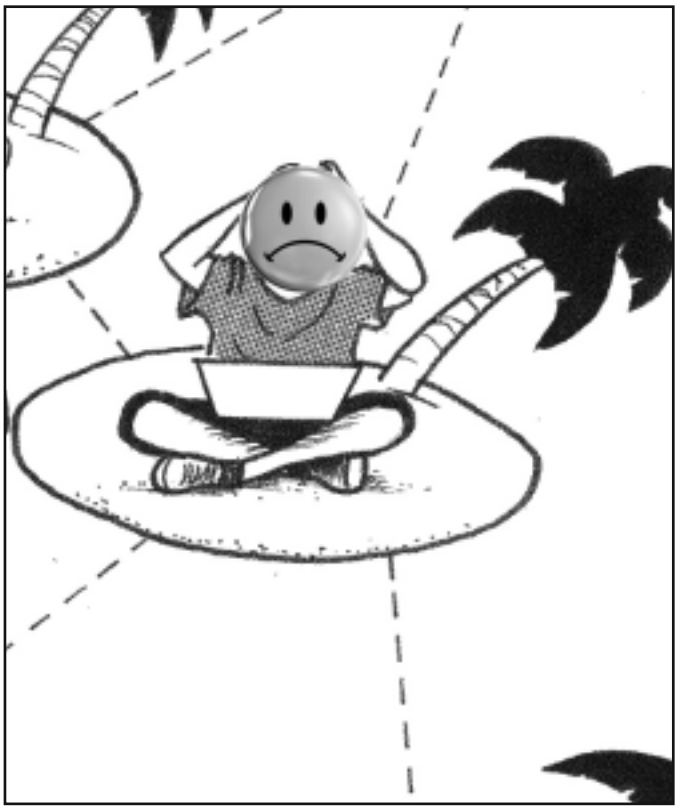
The alternatives that do a great job of empowering users in their privacy, security and anonymity will continue to improve, especially in terms of their accessibility. Their user base will grow, albeit not rapidly. There is a great chance that more and more social media niche services will arise (e.g. Stage32): social networks for particular groups of people with particular interests.

I think it's very unlikely that advertising and data-mining will somehow cease to be part of the social web. That's why Facebook will continue. Users will become increasingly aware that Facebook isn't free and that *they* are the product being sold. Will that make a huge difference? Probably not, since most users consider Facebook as a valuable asset in their social life, with their personal data part of the trade-off.

Twitter won't go the same way as Myspace either, since its users attribute so much immediate value to the service, and there is no end to news. Although the next big thing may be round the corner, most users are - and will remain to be - comfortable with their data bodies locked into these popular services.

Notes

* Unlike Us gathers artists, designers, scholars, activists and programmers interested in 'alternatives in social media'. Through workshops, conferences, online dialogues and publications, the international Unlike Us network analyzes the economic and cultural aspects of dominant social media platforms, such as Facebook and Twitter, and propagates the further development and proliferation of alternative, decentralized social media software. For more information, see http://networkcultures.org/wpmu/unlikeus/.



Tinker, tailor, cyber spy:

On modern surveillance technologies

*By **Rebecca Fisher***

The past ten years have witnessed a new kind of arms trade in off-the-shelf surveillance technology, spawning a booming billion-dollar industry and providing governments with tools to intercept entire populations. Relatively free from regulation or scrutiny, a number of IT companies have been making huge profits from developing scarily high-tech software to enable intelligence agencies, military forces, police authorities and private companies to silently, and on mass, intercept calls, track mobile phones and take over computers and/or capture their data. This software, developed largely in the US and Western Europe, is being sold to dictatorships and so-called democracies alike, with very little oversight.

What's on the market?

Documents relating to the vast array of products and services available and the companies providing them have been released recently by WikiLeaks in conjunction with Bugged Planet, Privacy International and media organisations from six countries.[1] This article analyses some of the data contained in these documents and profiles some of the companies behind them. The services provided by these companies can be grouped under five main areas: hacking, interception, data analysis, web scraping and anonymity.

Hacking

Hacking enables agents to break into computers and mobile phones, log keystrokes and access data. Companies developing these techniques often use 'malware' (software used to illegally steal people's personal or financial details). These 'trojans' “hijack individual computers and phones (including iPhones, Blackberries and Androids), take over the device, record its every use, movement, and even the sights and sounds of the room it is in.”[2] As offensive-security manager at HackingTeam SLR Marco Valleri puts it, the goal is to overcome the fact that most surveillance techniques are “useless against encryption and can't reach information that never leaves the device... We can defeat that.”[3]

One of the most notorious companies using such techniques is the UK's Gamma International, which has developed a range of products to grant clients access to personal computers, email, chats, Skype communications, social networking sites and mobile devices. The products work on most operating systems (Windows, Mac OSX and Linux) and bypass 40 regularly tested anti-virus programmes. All that needs to happen is to secretly infect a computer or device with this software, for which Gamma has developed a variety of methods, including falsifying updates of popular software in order to trick people into installing its programmes, or setting up fake websites which silently install the programmes onto visitors' computers. Links to these websites can be sent to a particular 'target' via a discussion board, for example, which would have been designed to catch their interest through previous profiling.

Another method, designed with intelligence agencies in mind, integrates Gamma's hacking tools within the Internet Service Provider itself, allowing Gamma to remotely infect particular websites, thereby installing the programmes on the computers of all those who visit the sites. Such websites can be selected according to specific criteria, for example those deemed 'government-offensive' or popular ones in certain communities. Once installed, the remote monitoring software can grant the client access to data about everything that the user is doing on the internet, including emails, web surfing, communications and even document transfers.[4]

Such methods can be employed not only against individuals but also on a mass scale. HackingTeam advertises its Remote Control System on the

grounds that it “can monitor from a few and up to hundreds of thousands of targets” and that the “whole system can be managed by a single easy to use interface that simplifies day by day investigation activities.”[5]

Of course, websites try to develop defences against such malicious malware. However, companies like Vupen Security SA of France employ teams of researchers dedicated to finding 'unpatched vulnerabilities', i.e. security holes that the manufactures are not yet aware of in software created by Microsoft, Adobe, Sun, Apple, Oracle, Novell and others. Vupen's marketing documents note that it is meeting law enforcement agencies' need for “the most advanced IT intrusion research and the most reliable attack tools to covertly and remotely gain access to computer systems.”[6]

With such fast-developing technology, it seems very little is safe from the rather innocuously named 'IT intrusion', i.e. cyberspace spying. The capabilities of these technologies is truly chilling. In the words of David Vincenzetti, chief executive of HackingTeam, “You can infect anybody on the Internet... When the infection has taken place, you get full control... and that means you can extract any information from that device.”[7]

Interception

Interception has developed into taking all the traffic from the internet and mobile phones, and sending it through devices that inspect packets of data, determine their content, detect patterns, and select what to copy for law enforcement agencies. As Brian McCann, the CEO of New Jersey-based OnPath Technologies Inc, says, “We can take a copy of everything coming through our switch and dump it off to the FBI.”[8]

Such devices are becoming smaller and smaller, including ones that can fit inside a rucksack, yet can still masquerade as legitimate mobile phone base stations, and therefore enable the interception and decryption of SMS messages and phone calls within a radius of several hundred metres.[9] According to Eric King from Privacy International, such devices are marketed as “perfect tools during public order situations – allowing law enforcement agencies to unmask protesters without them even knowing.”[10] Such technology also allows authorities “to track phone users’ movements in real-time, without having to request location data from a mobile phone carrier.”[11] Location tracking has long been used by law enforcement agencies, usually relying on triangulation to locate the phone, by which the strength of signals between phones and nearby mobile phone towers are evaluated and the phone's location determined.

Interception technologies have also developed to overcome people's use of encrypted communication. For instance, PacketForensics has developed 'man in the middle' programmes, in which the attacker is placed between two computers communicating, enabling the attacker to monitor or alter communications, insert malicious software into the data transmissions, or gain access to any security passwords they may be using. In this way, the difficult task of decryption seems to be unnecessary and, as PacketForensics boasts, “Your investigative staff will likely collect its best evidence while users are lulled into a false sense of security.”[12]

Companies are also developing so-called 'massive intercept' technology, at country level, which can capture vast amounts of data extremely quickly. UK-based Telesoft Technologies Ltd boasts that its “highest density optical passive probe” can provide “targeted or mass capture of 10s of thousands of simultaneous conversations from fixed or cellular networks for law enforcement or intelligence purposes.”[13] Telesoft would either “hand off 100% of the data to law enforcement agencies” or, helpfully, “filter the data by target information to any level as required.” As Eric King notes, technology to tap the undersea cables that convey all the data and phone traffic between continents enables the “mass surveillance of entire populations”.[14] US-based Glimmerglass Network is one of the pioneers in this field, specialising in monitoring the internet and telecommunications data passed via fibre-optic cables, including the massive amounts of data and phone traffic passing through international gateways and submarine cable landing stations. In addition, the company offers sophisticated technology to draw ties between people who are communicating with each other and even get details of their chats.[15]

Data analysis

All these massive amounts of data require sophisticated data analysis technology in order for it to be useful. Corporations have been quick to exploit this 'need', developing powerful software to filter, store and analyse data. For instance, S8 has developed a programme to analyse data gleaned from social networking

sites, called Social Network Analysis (SNA). This enables it to detect patterns, and thereby provide intelligence, about “the structure of the network and the importance of individuals within the network.” As the company's brochure notes, “Investigators are typically buried in volumes of data – SNA helps them put a structure around this turning it into useful information... investigators need new tools to both understand the patterns and relationships in the intercepted communications and to drill down and isolate individual communications relevant to the case.”[16]

Triangulating information from a variety of sources is used to build a fuller picture of a particular target or targets. Companies have even stepped in to facilitate high-tech and fast linguistic analysis. For instance, Italy-based Expert Systems has developed a specific programme, called Cognito, which “comprehends the meaning of information and finds hidden relationships, unlike traditional technologies that can only guess something using keywords.” As well as handling various different languages, the programme is able to differentiate between identical words but whose meaning changes according to context. Indeed, the programme is promoted for its being uncannily 'human' in its cognitive abilities: “Cognito understands the meanings of words – just as people do when they read.”[17]

Web scraping

Companies are also engaged in providing their clients with sophisticated technology for trawling publicly available sources on the internet, including government records, media reports, social-networking sites and other user-generated web content. This is called Open-Source Intelligence (OSINT) and is a crucial field to mine for information. In the words of Kapow Katalyst, “Mission critical data can reside in blogs, in news feeds, in social media.” Its software apparently enables clients to 'Harvest text in any language, images, audio, video from websites, blogs and social media,” while remaining “secure and non-attributable.”[18]

Technology is also available to trawl the 'Deep Web' or 'Invisible Web', that is, content on the internet that is not indexed by search engines and therefore much harder to find. Developed with governments in mind, this technology is now being marketed for commercial interests. BrightPlanet proudly notes it is “bringing its patented Deep Web harvesting technology to the commercial and research community through multiple service solutions,” including by trawling through the Deep Web, '*Proprietary* Data sources', 'Customers' Internal/*Private Data* sources' as well as 'the conventional *Surface Web*.”[19]

Whilst not hacking or intercepting private or classified information, this still yields a huge amount of personal information very quickly and is, therefore, of great use for companies, both for marketing purposes and to detect and spy upon anyone challenging their interests. Companies known to use such technology to profile anti-corporate activists include Agenda Security Services, Global Open, C2i, Inkerman Group and InQuire, among others.[20]

Anonymity

All this covert surveillance does not usually go down too well. For some investigations, secrecy is required, and a niche market has therefore developed for technology that hides the internet protocol (IP) addresses, allowing users to visit websites or build online profiles without disclosing their locations. Ironically, Ntrepid ION markets its software as a defensive measure against 'target websites' that employ surveillance techniques on government agencies: “Organizations that do not protect themselves are enabling criminals to uncover organizational affiliations, track online movement, and successfully counterattack based solely on the identification of the analyst's IP address.”[21]

The clients

So who uses these technologies? Most of this surveillance software is sold to governments – often called, rather euphemistically, 'law enforcement agencies' in company documents. But while much of the outrage focuses on its usage by commonly acknowledged repressive regimes, such as those of Egypt, Syria and Iran,[22] most of this technology is sold within so-called democratic states, such as the US and Western European countries, where the technology is first developed.

For instance, in 2011 it was revealed that London's Metropolitan Police had purchased new software made by Geotime that can track every movement a 'suspect' and their associates make in the digital world, displaying the results on a three-dimensional map.[23] The spying software, which is already used by the US military, gathers information from various sources including financial transactions, IP logs (internet usage), social networking sites, mobile phones and satellite navigation equipment.

The current UK coalition government, under pressure from the police and security services, has been pursuing this path further and is currently drafting legislation, originally penned by Labour in 2009 and dubbed as a 'snooping charter', to allow for the tracking of emails, text messages, Facebook and other internet use.[24] This seems an attempt to return to the days when we all used BT-owned landlines to communicate, allowing the police ready access to almost all communication in Britain. Now, “in the era of Google, Facebook and Twitter,” to quote Eric King, “the authorities have been cut off from significant chunks of people’s communications and a lot of data resides on foreign servers.”[25]

King describes this as “the kind of mass surveillance system favoured by Al-Assad, Mubarak and Gaddafi.”[26] The UK authorities are clearly emboldened by the use of social media tracking to facilitate convictions following the August riots, after which telecommunication companies such as Research in Motion (RIM), the makers of the BlackBerry, volunteered to 'help' the government identify their clients.[27] RIM has also negotiated to share BlackBerry Messenger data with the governments of India, Lebanon, Saudi Arabi and the United Arab Emirates.[28] This only goes to show how few scruples private companies have in relinquishing customer data to the state, and how much they can reveal even before using any high-tech surveillance technology.

However, companies often do not need to relinquish their information if technology is available to access it secretly. Skype has long been seen by activists as a secure way of communicating, as its powerful encryption technology makes it impervious to traditional wiretaps.[29] However, when Egyptian activists raided the headquarters of the state security agency in Cairo, they uncovered a secret memo about a trial taking place between August and December 2010 of a “high-level security system” made by Gamma, which reported “success in hacking personal accounts on Skype” and “recording voice and video conversations over the Internet”, as well as breaking into email accounts, tracking the location of a targeted computer and copying all of its contents.[30] The trial boasted of achieving “the successful penetration of their online organizational meetings... via encrypted Skype.” For the security forces, access to Skype calls was crucial because, as the memo states, it “counts as a safe and encrypted internet communication system to which most extremist groups have resorted to communicate with each other.” One activist, Basem Fathi, found files describing his love life which had been gleaned from intercepted emails and phone calls. Another, Israa Abdel Fattah, found in the agency file copies of her emails, transcripts of phone calls and text messages, and a list of companies where she had applied for jobs.

This was far from the only instance of multinational companies' meeting the spying needs of highly repressive regimes. In January 2011, shortly after the Egyptian uprising erupted, a report by Free Press revealed that Deep Packet Inspection (DPI) technology was sold to Egypt's main, state-owned telecommunications company by California-based company Narus.[31] Narus is best known for creating NarusInsight, a supercomputer system used by many governments and large corporations to perform mass surveillance and monitoring of public and commercial communications in real time. The technology, sometimes known as Semantic Traffic Analysis, is known for its ability to sift through vast quantities of information at very high speeds, identifying information packets 'of interest', with the ability to target customers by application (webmail, chat, e-mail client, Skype and so on) or by phone number, web address (URL), e-mail address, login account or keyword.[32] In 2006, the company's vice president for marketing, Steve Bannerman, told *Wired* magazine: “Anything that comes through [an IP network], we can record. We can reconstruct all of their e-mails along with attachments, see what web pages they clicked on, we can reconstruct their [Skype] calls.”[33]

Meanwhile, spyware containing a 'remote access tool' to remotely eavesdrop on calls and capture keystrokes was found to be distributed via a website named after the date the Libyan protests began. Other countries, such as Oman, Egypt, Iran and the United Arab Emirates block or partially block the use of Skype. And western companies, such as Narus and Bitek International Inc., both based in California, and German firm Ipoque GmbH, help out by providing them with products to detect and block any Skype usage. Bitek even admits it can capture Skype traffic and turn it over to governments for analysis. Similarly, Gamma, DigiTask GmbH, Hacking Team SLR and Switzerland's ERA IT Solutions AG have developed tools to eavesdrop on Skype calls, with Gamma and HackingTeam both marketing their software to governments outside Europe, including the Middle East. However, in Egypt at least, the dissenters seem to have won out for

now. The documents found in the raid stated that the Interior Ministry had decided to go ahead with the purchase of the Gamma system in December 2010, but that the deal had never gone through because, as Mr Kadry, Gamma's reseller, put it, Egypt's revolution derailed it.[34]

Popular pressure can have an impact in other ways too. For instance, when it emerged that French company Amesys had been selling spyware to Gadhafi, it was forced to sell off its internet-interception equipment business after the Libyan revolution suddenly made this collaboration in repression a PR disaster for the company. As Ameys admitted, “The contract was concluded at a time when the international community was in the process of diplomatic rapprochement with Libya.”

But companies are not always required to take such scruples in who they sell their spyware to. Firms wishing to export surveillance technologies from Europe or the US do not currently require any sort of export licence. And when restrictions are in place, such as on exports to Syria, which is subject to strict trade sanctions, these can be overcome by selling to a re-seller company, in somewhere like Dubai, where an annual ISS World conference has “long served as a chance for Middle East nations to meet companies hawking surveillance gear.”[35]

Although the US government requires re-export licences for controlled devices, these rules seem to be rarely enforced, and companies claim not to track where their technology goes after an initial, legal sale.[36] This seems to be how equipment made by US company BlueCoat, which provides internet-blocking technology, found its way to Syria and was used to block sites such as the Muslim Brotherhood website and the-syrian.com, a website dedicated to news about the uprising. BlueCoat claims its devices were destined for the Iraqi government and is not aware of how they got to Syria. To quote Eric King again, “the complex network of supply chains and subsidiaries involved in this trade allows one after the other to continually pass the buck and abdicate responsibility.” Jerry Lucas, president of TeleStrategies Inc and organiser of the surveillance conference in Washington D.C. in October 2011, is particularly candid: “We don't really get into asking, 'Is this in the public interest?'”[37]

What can be done?

The result of all this explosion in surveillance technologies is effectively the militarisation of the Internet and mobile phone communications. In the words of Peter Fain, member of the hacktivist group TeleComix, which first exposed BlueCoat technology in Syria, “State surveillance using these devices has real world consequences... these machines can be as dangerous as a club or gun.”[38]

Still, it is important to note that such technologies are not invincible. As Eric King writes, “The surveillance systems used are very sophisticated, but they're not perfect. For example, creating multiple email addresses using different pseudonyms, and using online anonymity tools like Tor, will significantly enhance your security and privacy, while leaving your mobile phone at home when you attend protests or meetings will help prevent the automated tracking of your location.”

Company Profiles*

Gamma Group

Fellows House, 46 Royce Close, West Portway Industrial Estate, Andover, Hants, SP10 3TX, UK.

Sells: trojans/intrusive software, internet monitoring/mass surveillance, SMS monitoring, speech analysis/voice recognition.

The company's primary surveillance product is called FinFisher IT Intrusion. When inserted into a target's computer, this can grant access to its files and activities, and can even activate the computer's webcam and microphone to watch their target. It boasts that this can allow “a government agency to... take control of the target.” The technology was found to be used by Mubarak's regime in Egypt, though the company denies selling it directly to the Egyptian government.

Telesoft Technologies Ltd

Observatory House, Blandford, Dorset, DT11 9LQ, UK.

Sells: Internet monitoring/mass surveillance, SMS monitoring.

Telesoft Technologies specialises in 'massive

intercept' monitoring, boasting that it can offer "targeted or mass capture of tens of thousands of simultaneous conversations from fixed or cellular networks."

QinetiQ

QinetiQ Cody Technology Park, Ively Road, Farnborough, Hampshire, GU14 0LX, UK.

Sells: Internet monitoring/mass surveillance.

QinetiQ manufactures cyber surveillance products, claiming it provides "commercial organisations, national infrastructure utilities and government agencies" with tools to "protect themselves against crime, insider threats, terrorism and espionage." Formerly part of the Ministry of Defence, the company has close government connections and, in February 2011, it was part of a trade delegation to Kuwait led by David Cameron and defence contractors BAE Systems and Thales UK.

Cobham Plc

Brook Road, Wimborne, Dorset, BH21 2BJ, UK.

Sells: SMS monitoring.

Cobham offers a system to identify and track a target through their mobile phone signal. In 2009 it won a Queen's Award for Enterprise for International Trade after trebling the size of its overseas exports in three years. The company has four divisions employing over 12,000 people on five continents, with customers and partners in more than 100 countries and annual revenue of £1.4bn. Its advanced surveillance technologies allow an agent to lock onto a target's mobile phone and activate a "silent" call to keep the device "under their control", or continually under supervision.

Detica

Surrey Research Park, Guildford, Surrey, GU2 7YP, UK.

Sells: Analytics.

Deica is part of Britain's largest defence contractor, BAE Systems, and is "leading specialist in data collection and analytics, situational awareness and decision-support, and secure communication." Its analysis product, NetReveal, enables the ''rapid analysis of significant volumes of unstructured or semi-structured documents." It was also behind the UK government's 2008 initiative Intercept Modernisatio Program (IMP), which aimed to expand the government's capability for interception and storage of communication data. The programme was dropped by the Labour government but has since been revived by the Con-Dem coalition government. The proposal includes the collection of data on phone calls, emails, web browsing and chatroom discussions. Detical also came under fire when questioned in parliament whether its equipment was being sold in Tunisia. Baroness Wilcox, under-secretary for the Department of Business, Innovation and Skills replied that Detica did not need permission to export this kind of equipment under the current UK export control regime and "the Government therefore have no information on what has been sold to the Government of Tunisia by Detica."

Datong

1 Low Hall Business Park, Low Hall Road, Leeds, LS18 4EG, UK.

Sells: SMS monitoring

Datong provides mobile intelligence and signals intelligence abroad, including 'IMSI catchers' – a technology to remotely track mobile phones. In October 2011 it emerged that the Metropolitan Police had paid Datong £143,455 for equipment to track and intercept thousands of mobile phones in a targeted area via masquerading as a mobile phone network. The company already sells its technology to the US government and lists partners in Bangladesh, Colombia, Indonesia, Malaysia, Mexico, Thailand and Vietnam.

Sophos Plc

The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.

Sells: Internet monitoring/mass surveillance.

Trumpeted by the UK Trade & Investment (UKTI) as one of Britain's "leading technology companies", Sophos is a major player in the UK's computer security industry. It produces IT security such as antivirus systems, encryption and web and spam filtering, all of which could double as web-blocking software. For instance, hardware produced by German computer-security company Utimaco, which Sophos bought in 2009, was found to be used by the Assad regime to crack down on Syrian dissidents.

References

[1] ARD in Germany, The Bureau of Investigative Journalism in the UK, The Hindu in India, :'Espresso in Italy, OWNI in France and the Washington Post in the US. See here for all the documents: http://wikileaks.org/The-Spyfiles.html. In addition, in November 2011 the Wall Street Journal published documents from a corporate surveillance conference held near Washington D.C. see here: http://projects.wsj.com/surveillance-catalog/).
[2] http://wikileaks.org/the-spyfiles.html
[3] Quoted in http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
[4] See http://wikileaks.org/spyfiles/files/0/296_GAMMA-201110-FinFly_Web.pdf and http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[5] See http://wikileaks.org/spyfiles/files/0/296_GAMMA-201110-FinFly_Web.pdf and http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[6] http://projects.wsj.com/surveillance-catalog/documents/267761-documents-265202-vupen-exploits/#document/p1/a38929
[7] Quoted in http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html
[8] http://projects.wsj.com/surveillance-catalog/documents/267794-documents-266211-onpath-technologies-lawful/#document/p1/a39169
[9] http://blog.soros.org/2012/02/the-spy-files-an-interview-with-eric-king/
[10] Ibid
[11] http://www.thebureauinvestigates.com/2011/12/01/surveillance-debunked-a-guide-to-the-jargon/
[12] http://wikileaks.org/spyfiles/files/0/276_PACKETFORENSICS-2009.pdf
[13] http://projects.wsj.com/surveillance-catalog/documents/267027-telesoft-technologies-hinton-5000-interceptor/
[14] http://blog.soros.org/2012/02/the-spy-files-an-interview-with-eric-king/
[15] http://projects.wsj.com/surveillance-catalog/documents/266923-track-1-thursday-glimmerglass-networks/
[16] http://wikileaks.org/spyfiles/files/0/207_SS8-SOCIALNETANALYS-201110.pdf
[17] http://projects.wsj.com/surveillance-catalog/documents/266173-expert-system-semantic-intelligence/#document/p1/a38606
[18] http://projects.wsj.com/surveillance-catalog/documents/266252-kapow-katalyst-for-osint/#document/p1/a39036
[19] http://projects.wsj.com/surveillance-catalog/documents/266243-brightplanet-the-deep-web/#document/p1/a38911
[20] http://www.corporatewatch.org/?lid=3869
[21] http://projects.wsj.com/surveillance-catalog/documents/267021-ntrepid-ion-mission-research-and-targeting/#document/p2/a39038
[22] See, for example, http://www.thebureauinvestigates.com/2011/11/30/uks-top-spies-approved-export-of-surveillance-technology-to-iran/
[23] http://www.guardian.co.uk/uk/2011/may/11/police-software-maps-digital-movements/print
[24] http://www.guardian.co.uk/world/2012/may/09/snoopers-charter-crime-bill-facebook
[25] http://www.thebureauinvestigates.com/2012/04/02/analysis-the-british-governments-new-plans-for-mass-surveillance/
[26] http://www.thebureauinvestigates.com/2012/04/02/analysis-the-british-governments-new-plans-for-mass-surveillance/
[27] http://blog.soros.org/2012/02/the-spy-files-an-interview-with-eric-king/
[28] Ibid
[29] http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html
[30] Ibid
[31] http://www.freepress.net/press-release/2011/1/28/questions-raised-about-us-firms-role-egypt-internet-crackdown
[32] For more one the company and its products, see http://www.corporatewatch.org/?lid=3880
[33] http://www.wired.com/science/discoveries/news/2006/05/70914
[34] Ibid
[35] http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
[36] http://blog.soros.org/2012/02/the-spy-files-an-interview-with-eric-king/
[37] Quoted in http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
[38] http://www.thebureauinvestigates.com/2011/10/23/us-technology-used-to-censor-the-internet-in-syria/

* Information based on http://bigbrotherinc.org/v1/United%20Kingdom/ and http://www.thebureauinvestigates.com/2012/04/02/analysis-the-british-governments-new-plans-for-mass-surveillance/.

Anonymous

Anonymous is difficult to define. For some, it is a tactic; for others, a movement, a collective, a hacker group or a vigilante group. The most convincing description seems to be a "culture... nascent and small", as Quinn Norton writes, but one with "its own aesthetics and values, art and literature, social norms and ways of production, even its own dialectic language."[1] It has developed into a substantial and effective political force, combining spectacle with infrastructure hacking to produce new ways to attack governments and corporations, principally for suppressing freedom of speech and protest. In this article, ***Tom Anderson*** *and* ***Rebecca Fisher*** *delve into Anonymous, bringing out some of its defining characteristics and exploring its evolution into a powerful force against corporate and state power.*

campaign spotlight

"Anonymous is a banner which any citizen can fly… This means you are anonymous."[2]

"Anonymous does not exist... It is just an idea; an Internet meme...

It is a beehive where the queen is missing. Yet buzzing with activity."[3]

Tactics

Anonymous has launched online attacks on websites and servers all over the world, made occasional forays into street protest and offline direct action, and tackled a wide range of issues and targets, from cults to law enforcement agencies and from government departments to drug cartels and multinational corporations. It has also employed a variety of tactics in its actions against such targets, including:

- **Pranks**, such as bombarding a target with phone calls and emails, phoning in fake pizza deliveries, faxing black pages of paper to waste toner and so on.[4]
- **Distributed Denial of Service (DDoS) attacks**, which involve flooding a website with a large number of hits to stop it working. This has sometimes been done by a number of activists each pointing a 'load testing' device, a program designed to test whether a server can cope with a high volume of hits, at a target server.[5]
- **Doxing**, or gathering information about a target from the internet to use it against it. This has sometimes involved seizing private information.[6]
- **Data dumps**, or taking private information about a target and making it public.[7]
- **Protest and offline direct action** – Anonymous 'operations' have included mass street protests and occupations of buildings, for example during the anti-Scientology campaign and OpBart.[8]

Anonymous-style tactics are not new, of course. The idea of disguising identity in order to express dissent has been used throughout history, and more recently as a staple of anti-capitalists, from the Zapatista rebellion in Chiapas to the use of black bloc tactics on street demonstrations across Europe. Hacking is also not a new practice. However, Anonymous actions are identified by shared imagery and ideas: the masks, hyperbolic video communiqués dictated by a computer-generated voice, the sign-off ("Anonymous does not forgive", etc) and a commitment to freedom of information.

Tricksters

In order to understand the weird world of Anonymous – their love of cats, their unashamed use of offensive language, their incessant pranking – it is important to understand the archetype of the *trickster*. This is the term used in mythology and folklore to denote a figure or spirit who plays tricks, and otherwise disobeys normal rules and conventional behaviour, in order to expose contradictions and initiate change; who rejects traditional morality by embodying neither hero nor villain status. As Norton writes in *Anonymous 101: Introduction to the Lulz*, "One minute, the loving and heroic trickster is saving civilization. A few minutes later the same trickster is cruel, kicking your ass and eating babies as a snack."[9] In the Anonymous culture, these qualities are borne out in primacy of pranking and disregarding accepted morality. "The trickster as myth proved so compelling that the network made it real. Anonymous, the net's trickster, emerged like a supernatural movie monster out of the misty realm of ideas and into the real world."[10]

One of the most fundamental elements in Anonymous' trickster nature is the concept of the 'lulz'. A corruption of LOL (online abbreviation for 'laughing out loud'), the lulz mean doing something weird or unexpected for the sake of personal comic enjoyment. But it is a particular kind of humour, as Norton explains: “The lulz is laughing instead of screaming... It's not the anaesthetic humor that makes days go by easier; it's humor that heightens contradictions. The lulz is laughter with pain in it. It forces you to consider injustice and hypocrisy, whichever side of it you are on in that moment.”[11] Over the years, this trickster culture has evolved from funny pranks to (still funny) acts of political disruption and resistance.

Origins

Anonymous has its roots in the hacking and pranking culture within Internet Relay Channels (IRC), EFnet and the 1990s hacker scene. It was born on a website called 4Chan, founded in 2003, which developed an anonymous forum where users could not be traced nor their posts archived. A particular section of the site, known as the /b/ board, developed to be explicitly about anything and everything. Norton argues that this functioned as a kind of collective identity: “the collective unconscious version of the place from which the base drives arise,” and in which anything was permitted, from the highly offensive to the sweet and innocuous.[12] For Norton, the forum has “a kind of innocence and purity” in which “terms like 'nigger' and 'faggot' are common” and act to discourage those not familiar with the culture: “These words are heads on pikes warning you that further in it gets much worse, and it does.”[13] /b/ seems to provide a way for people to say what they like without censorship and, while sometimes this includes offensive material, often it is sweet and harmless, such as “talk[ing] about 'My Little Pony: Friendship is Magic'.”[14]

For some, this offensive language, which still permeates forums used by Anonymous activists (or anons) such as whyweprotest.net,[15] reflects an amoral, nihilistic streak within the culture of Anonymous. Whether or not the language signifies an underlying amorality, its use sits uncomfortably with many anons, particularly those who are increasingly moving into political campaigning and interactions with the wider activist community. But it is this 'anything goes' attitude that typifies a great deal of Anonymous culture and is key to understanding anons' actions, both in terms of their trickster sense of humour and in their emphasis on freedom of speech.

This identity seems to have “spilled into the rest of the net” when Anonymous started its 'raids', that is, collectively coordinated attacks on targets for any perceived slight, or just for fun, without warning and without providing the victims with any means of defending themselves.[16] Pursuing a slightly chaotic and often controversial trajectory, the targets chosen and tactics used against them have steadily become more political.

When a video of Tom Cruise manically proselytising for Scientology was leaked out, the highly litigious 'church' tried to get it removed, and Anonymous launched into action to keep it online. To do this, they created their first 'op' (short for operation), called Project Chanology. Norton argues that this “marked both the birth of political consciousness for Anonymous, and the development of its methods of taking mass action.”[17]

To the dismay of some within Anonymous, this developed into a moral campaign, taking the high ground against the Church of Scientology for hurting people, taking their money while promising to look after and teach them. For many veterans, this was the opposite of the lulz, and a sign of the 'cancer' that was killing /b/. But the self-styled 'moralfags' within Anonymous left the internet and set up meetings all over the world. In February 2008, anti-Scientology protests were held in several cities, during which participants hid their identities by wearing identical Guy Fawkes masks made famous by the character V in the graphic novel *V for Vendetta* and worn by the character Epic Fail Guy on 4Chan.[18] This morphed into a relentless attack on the Church of Scientology, encompassing a broad range of protest and disruption techniques which Anonymous called 'raep', a misspelling of 'rape', replicating the use of offensive language that had been prevalent on /b/. The protests multiplied and developed from 2010 onwards, including the creation of WhyWeProtest.net, an online social network and forum site that currently has public forums on freedom of information, anti-Scientology campaigns, the Occupy movement and the struggle against the Iranian regime.

These tactics worked particularly well against the Church of Scientology, whose main defence against criticism has always been legal action. Litigation was impossible with no name to take to court. Previously, Scientology had also attempted to ruin the reputation of its detractors, but this could not work against Anonymous either. As Norton writes, “Anonymous didn't care. Call them rapist and they'd laughingly tell you they were child rapists... Anonymity and the

'words will never hurt me' ethic that arose out of the aesthetics of extremes on 4chan made them immune to the Church's arsenal."[19]

Operations

Despite eliciting negative reactions from some anons, such concerted attacks as those demonstrated in Operation Chanology, combining a moral standpoint with a lulz mentality, took root within the Anonymous culture. In 2010, anons became involved with two glabal struggles for online information freedom. Indeed, if Anonymous can be said to have any shared philosophy, it is one about the freedom of information. WhyWeProtest has this to say about the issue:

"*A common thread that binds many internet users and impels them toward Anonymous is the concept that information, by its nature, is free; and that communication should be unfettered. The open sharing and expression of ideas and opinions, however controversial or divergent, is the cornerstone of all free societies. This ability empowers individuals to determine their own destinies; justice is possible only when the influential cannot force others to remain silent about abuse*."[20]

Firstly, the hive mind of Anonymous coalesced into a protest against what it saw as attempts by the Hollywood studios to not only write copyright laws that hampered online freedoms, but use illegal techniques, such as DDoSing, which anons had been jailed for. When it appeared that Indian company AiPlex had been contracted by the Motion Picture Association of America (MPAA) to send out take-down requests to piracy sites and DDoS those that refused to comply, such as The Pirate Bay, Anonymous created Operation Payback, in which they promised to "prevent users to access said enemy sites [those of the the Recording Industry Association of America (RIAA), the MPAA and AiPlex] and we will keep them down for as long as we can." This was because they were "tired of corporate interests controlling the internet and silencing the people's rights to spread information, but more importantly, the right to SHARE with one another."[21]

During Operation Chanology, anons had hit upon a new and formidable cyber weapon –the ludicrously named Low Orbit Ion Cannon (LOIC) – which enables a computer programmer to test a website's capacity by loading it with traffic. LOIC is innocuous enough in itself, but not when enough people download it and send vast amounts of traffic to a single target, often causing the site to be taken down. This was applied against the websites of AiPlex and MPAA, and the sites were indeed removed soon.

One of the most significant results was to generate a lot of media attention, to increase the numbers of those taking action via Anonymous, and to ensure that now the anons who wished to use the Anonymous banner for political purposes rather than just the lulz were in the majority. The Anonymous hive mind started to gain an appetite for effective political action.

This appetite was again whetted later in 2010 when the US government cracked down on WikiLeaks. Following the release of hundreds of thousands of diplomatic cables, anons jumped into action, using the LOIC to attack companies that had complied with the US government and ceased providing services to WikiLeaks. These included Amazon, Mastercard, Visa and Paypal.[22] The attacks became known as Op Avenge Assange, which proved compelling yet confusing to the mainstream media. Many missed the fact that these attacks did not actually manage to disrupt the functioning of these target companies for very long, but managed to increase the attacks' effectiveness by leading people to believe that their Visa or Mastercards had been rendered unusable.[23] Meanwhile, anons continued to help keep the leaked cables available all over the world by mirroring them on other servers and keeping track of where they had been censored.[24]

Freedom Ops

As the popular uprisings in the Middle East and North Africa began at the end of 2010, anons saw a way to have a much wider impact. In the characteristic monotone computer voice, an Anonymous press release stated: "Anonymous has heard the cries for freedom from the Tunisian people and has decided to help them win this battle against oppression... Any organization involved in censorship will be targeted. Attacks will not stop until the Tunisian government hears the calls for freedom from its own people... This is not a battle which is waged for you [the Tunisian people] alone but to serve as a precedent and statement to the world. We unite to send a message that we in fact are not simply quiet citizens who can be chocked and peddled into submission."[25]

Thus OpTunisia was developed, with the aim of launching DDoS attacks on Tunisian government targets and communicating with Tunisian dissidents, distributing information on the

uprising and disseminating advice and resources to help circumvent Tunisian state e-security measures and network securely online. As one anon reported, the following message accompanied one of the 'digital care' packages to Tunisia: “This is your revolution. It will neither be Twittered nor televised or IRC'ed. You must hit the streets or you will loose [sic] the fight. Always stay safe, once you got [sic] arrested you cannot do anything for yourself or your people. Your government is watching you.”[26]

As protests kicked off in Cairo's Tahrir Square in 2011, OpEgypt was launched with similar aims and objectives. Since then, a host of ’Freedom Ops' have been developed for countries all over the world, including Britain, Italy, Ireland, the USA, Venezeula, Brazil, Syria, Bahrain, Yemen, Libya and more.

One feature of these 'Freedom Ops' was spreading information about internet security to grassroots movements. Disseminating advice on how to express dissent online without being identified by the authorities is a vital way in which online activists can show solidarity with grassroots movements expressing anti-state and anti-corporate dissent. In 2011, those who had organised dissent using corporate-controlled social networks, from Tahrir Square to the British summer riots, faced arrest and prosecution after being identified from Facebook, Twitter and so on. The idea of mass secure networking is certainly a radical one.

Later in 2011, anons targeted Sony with DDoS attacks in protest at a lawsuit the company had brought against the person who had provided the means to re-enable the possibility of installing Linux on Sony's PlayStation 3, which the company had removed.[27] Anons DDoS'ed Sony websites and other hackers, not necessarily associated with Anonymous, hit the PlayStation network and Sony Online Entertainment Network. The Sony Play Station Network was down for almost a month in April-May 2011, and its stock price fell from $31 per share to just over $25.[28]

Anonymous' activities have not been confined to cyberspace, however. In August 2011, the Bay Area Rapid Transit Authority (BART) in San Francisco shut down cellular communications during an anti-BART Police protest in relation to the shooting of a homeless man named Charles Hill in July that year. Anonymous soon heard about the events and formed OpBart, during which the insecure BART websites were mercilessly hacked and large amounts of information stolen from their servers. This created a media storm, particularly when anons came off the internet and onto the streets in masked protests.[30]

In many ways, this operation lay the ground for Anonymous' most concerted political intervention yet. As OpBart died down, Occupy Wall Street was just beginning, and many within Anonymous felt a great affinity with the Occupy movement. As Norton writes, “In the Occupy movement, Anonymous seemed to find a body its peripatetic spirit could inhabit.”[31]

Longcat, one of the many cat-based internet phenomena popular with Anonymous

In Winter 2011, an Anonymous cell stole thousands of documents, including credit card information, from Strategic Forecasts Ltd (Stratfor). Stratfor has provided intelligence analysis to the US military and many private companies since 1996.[32] As one participant noted, “They [Stratfor] promote global market stability, whereas we want financial meltdown... It's about creating an egalitarian society without bosses or masters, it's about forcefully redistributing the wealth and power in society.”[33]

In January 2012, it was claimed that the hacking had compromised many of the top 100 US government contractors. This has been particularly embarrassing for a company like Stratfor, which makes security its business. Anonymous claimed the company had not encrypted its data,[34] and used stolen credit card data to make large donations to charities such as the Red Cross, CARE and Save the Children. The charities later begged for hackers not to make donations through fraud as they could be charged a penalty.[35]

Most recently, in May 2012, online Anonymous attacks have been made against the government of Quebec, in protest at its “opting to assassinate the right to protest by adopting an emergency law to try and stifle protests against the tuition hikes.”[36] Hackers successfully brought down 13 government and police websites as part of OpQuebec.[37] This seems to have coincided with a recent trend for Anonymous attacks to broaden out from internet freedoms to the role of

police and other state forces in suppressing freedom to protest. As one participant notes, “We thought we had every right to gather in public parks, to speak our demands. And they systematically targeted us for elimination... So we decided it was time to coordinate a raid of our own.”[38]

Beyond Anonymous

Anonymous-style tactics can be an important weapon in the anti-corporate campaigning arsenal. However, these tactics, as with any other tactic, can be employed for both good and bad. Doxing has been used by corporations to gather information on activists for decades. In 2012, the Anonymous brandname itself was appropriated by an anti-abortion campaigner to target an abortion provider.[39]

The breadth and internationalism of Anonymous’ actions is to be admired. The tactics have been shown to have an appeal that cuts cross cultural and social frontiers. Indeed, anons are known to exist in many countries including the US, France, Chile, Argentina and Spain. However, there have also been concerted efforts by these countries to target them. Anonymous is currently being targeted by US law enforcement agencies, as well as the INTERPOL,[40] in the hope of stopping the hacking activities by arresting key figures in the network.

It certainly seems that, for now, the unashamedly political ranks of Anonymous are winning out over those who wish to concentrate on the lulz. In so doing, they have undoubtedly served to firmly embed the use of hacking tactics in a broad range of anti-state and anti-corporate struggles. The strength of Anonymous seems to reside in its leaderless, protean nature, which ensures it can both reflect the biases of its participants and quickly react to events. It is difficult to say how this new world of mass 'hacktivism' will develop; whether or not Anonymous will continue to evolve or fade into insignificance. But while it continues to combine humour and spectacle with political effectiveness, and to change form and direction, Anonymous remains not only hard to categorise but even harder to control.

Notes

[1] Quinn Norton, 'Anonymous 101: Introduction to the Lulz', Wired, November 8, 2011, http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1
[2] http://www.youtube.com/watch?v=BFLaBRk9wY0
[3] http://www.youtube.com/watch?v=7cqP8qqqfI0
[4] See, for example, http://www.nbcnewyork.com/the-scene/archives/Scientology-Protester-Greased-Up-and-Covered-In--Pubes.html
[5] Quinn Norton, 'Anonymous 101 Part Deux: Morals Triumph Over Lulz', Wired, December 30, 2011, http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux/all/1
[6] See, for example, http://www.thetechherald.com/articles/The-FBIs-warning-about-doxing-was-too-little-too-late
[7] http://www.eweek.com/c/a/Security/Anonymous-LulzSec-Dump-Data-from-70-Sheriffs-Offices-547474/
[8] Offline protest has been used extensively in the anti-Scientology campaign. See, for example, http://www.schnews.org.uk/archive/news6321.htm and http://www.nbcnewyork.com/the-scene/archives/Scientology-Protester-Greased-Up-and-Covered-In--Pubes.html
[9] Norton, 'Introduction', ibid.
[10] ibid.
[11] ibid.
[12] ibid.
[13] ibid.
[14] ibid.
[15] For example, in one thread on Whyweprotest.net, one contributor uses the words “faggot” and “retarded”, while another comments: “this thread gave me aids”. The authors are not rebuked for their use of language. See https://whyweprotest.net/community/threads/why-the-guy-fawkes-masks.63520/.
[16] Norton, 'Introduction', ibid.
[17] ibid.
[18] http://knowyourmeme.com/memes/epic-fail-guy
[19] Norton, 'Introduction', ibid.
[20] https://whyweprotest.net/freedom-of-information/
[21] Norton, 'Part Deux', ibid.
[22] http://www.corporatewatch.org/?lid=3858
[23] Norton, 'Part Deux', ibid.
[24] ibid.
[25] http://www.youtube.com/watch?v=BFLaBRk9wY0
[26] Quinn Norton, '2011: The Year Anonymous Took on Cops, Dictators, and Existential Dread', Wired, January 11, 2012, http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/all/1
[27] http://www.youtube.com/watch?v=2Tm7UKo4IBc
[28] Norton, '2011', ibid.
[29] http://www.wired.com/threatlevel/2011/08/subway-internet-shuttering/
[30] Norton, '2011', ibid.
[31] ibid.
[32] http://www.wired.com/threatlevel/2011/12/antisec-hits-private-intel-firm-million-of-docs-allegedly-lifted/. See also http://www.stratfor.com/about-us
[33] Norton, '2011', ibid.
[34] http://edition.cnn.com/2011/12/26/tech/web/anonymous-hack-stratfor/
[35] There are several claims, from sources claiming to be Anonymous, that the Stratfor hack was not the work of Anonymous. See, for instance, http://pastebin.com/8yrwyNkt.
[36] Quoted in http://www.montrealgazette.com/news/Hacker+collective+Anonymous+backs+Quebec+students/6668080/story.html
[37] ibid.
[38] http://www.wired.com/threatlevel/2011/12/antisec-hits-private-intel-firm-million-of-docs-allegedly-lifted/
[39] http://www.theargus.co.uk/news/9582759.Hacker_targets_abortion_clinic/
[40] http://www.interpol.int/News-and-media/News-media-releases/2012/PR014