Edith Cowan University

From the SelectedWorks of David M Cook

2014

Twitter Deception and Influence: Issues of Identity, Slacktivism, and Puppetry

David M Cook, *Edith Cowan University*
Benjamin Waugh
Maldini Abdipanah
Omid Hashemi
Shaquille Abdul Rahman

Available at: https://works.bepress.com/david_cook/15/

Twitter Deception and Influence: Issues of Identity, Slacktivism and Puppetry

David M. Cook[1,2], Benjamin Waugh[1], Maldini Abdipanah[1], Omid Hashemi[1], and Shaquille Abdul Rahman[1]
[1]Edith Cowan University School of Computer and Security Science
[2]ECU Security Research Institute
d.cook@ecu.edu.au

Abstract

There is a lack of clarity within the social media domain about the number of discrete participants. Influence and measurement within new media is skewed towards the biggest numbers, resulting in fake tweets, sock puppets and a range of force multipliers such as botnets, application programming interfaces (APIs), and cyborgs. Social media metrics are sufficiently manipulated away from authentic discrete usage so that the trustworthiness of identity, narrative and authority are in a constant state of uncertainty. Elections, social causes, political agendas and new modes of online governance can now be influenced by a range of virtual entities that can cajole and redirect opinions without affirming identity or allegiance. In the advent of the 2013 Australian Federal Election, the open source Twitter activity for the two main opposing political leaders was examined in order to determine the manner in which information was diffused. The results showed phony online personas, fake bots deploying automated Twitter dissemination, and deceptive Twitter strategies. New media tolerates slacktivism, where Twitter users mistake auto-narrative for genuine political sentiment. This study demonstrates the need to increase legitimacy and validity in micro-blogging forms of new media and the need for multi-factor authentication.

Keywords
Twitter, sock puppets, fake personas, botnets, social media, slacktivism, meat-puppets

INTRODUCTION

Background to Twitter

As an online social media micro-blogging service deploying short messages of 140 characters or less called '*tweets*', Twitter incorporates two key methods of influence (Lloyd, 2012; Twitter, 2013). The first is the practice of '*re-tweeting'* other people's tweets, demonstrating interest and confirming (at some level) support for the narrative's existence and continuance online. The second expression of impact comes from the ability to overtly '*follow*' other Twitter entities. This provides immediate access to preferred content and affirms an interest in both the original tweeter and any associated persons' narrative (Chu, Gianvecchio, Wang, & Jajodia, 2010; Kwak, Lee, Park & Moon, 2010). Retweets command additional authority and leverage to original tweets because they transmit an original message from a source, whilst simultaneously conferring tacit acceptance of successive retweeted messages (Parmelee & Bichard, 2013).

Influence and Legitimacy

Twitter messages exhibit information that stimulates mass audiences to follow, retweet, and recite brief narrative descriptions (Jansen, Zhang, Sobel, & Chowdury, 2009). Political personalities and their respective causes command considerable authority and influence through the repeated devolution of twitter narratives (Papacharissi, 2010; Cogburn & Espinoza-Vasquez, 2011). Elections in Africa and the Middle East (notably Iran, Egypt and Nigeria) have all undergone striking moments of authority and persuasion from the use of Twitter (Solow-Niederman, 2010; Hamdy, 2010; Howard, 2011). From a global and national security outlook the capability to awaken and rouse the wider populace according to political will signifies sizeable threat (Papacharissi & Oliviera, 2012; Howard, 2011). The legitimacy of that power and influence is therefore of interest, particularly if augmentation of the range, frequency and impact of these messages can be interfered with. Whilst it is possible to intercept another's Twitter account and to deploy non-genuine posts (Jeffries, 2010), such false messages are straightforwardly exposed and simply renounced (Cao, Sirianos, Yang & Pregueiro, 2012: Zhang, Hong & Cranor, 2007). Consequent narratives can fortify an individual's more accurate objectives (Wilson, 2011). Although the legitimacy of original tweets may be trusted as time progresses, the authority, cogency, and truthfulness of large-scale multiple retweeted communications only receives momentary and fleeting examination (Jewitt, 2009; Papacharissi, 2010). Twitter's own estimation in September 2013 was that there were roughly 10.75 million non-genuine Twitter accounts (D'Yonfro, 2013) in the form of fake followers, or accounts associated with individuals with numerous personas (USSEC, 2013; Yarow, 2013). The

capability for Twitter to be harnessed in order to influence the outcomes of electoral decision making, underscores the need to determine authentic identities from non-genuine multipliers (Lloyd, 2012; Parmelee & Bichard, 2013; Waters & Williams, 2011).

Fake Tweets: Malfeasance or Idle Acceptance

The contested issue of whether the use of multiple personas should remain legally permissible continues to emphasize rights issues about truth versus free speech (Parmelee & Bichard, 2013). If a person decides to deploy several online personas and present them as discrete entities on Twitter, does the general public have the right to know that multiple guises are being set up? Sock puppetry has been deployed by individuals for centuries as a method to mislead and manipulate the beliefs, judgments and actions of others (Chu, et al., 2010). The term was initially expressed in a web-based context in 1993 when an online chat room audience exposed one of the participants trying to influence the narrative conversation by using a second online persona under a false pseudonym (Rollins, 1993). Since then, the practice of sock puppetry has been documented in online business promotions (Streitfield, 2012), political support and enticement (Cogburn & Espinoza-Vasquez, 2011), and terrorist coercion (Conway, 2012). Establishing the identity of online personas would assist in adding meaning and credibility to social media discourse.

Twitter has now been repeatedly used in the political elections of nation states, and for both the stability and upheaval within regions and zones as an authoritative vehicle for persuasion (Waters & Williams, 2011). The medium is useful in countries where the normal means of media becomes blocked or muted for those in opposition to government (Bartlett, Birdwell, and Littler, 2011) and is helpful in elected nations where minority voices attempt to be heard (Gleason, 2013). The size of an organization need not reflect the level of influence delivered through Twitter. The ability to deploy force multipliers within Twitter traffic means that the retweets of a few can replicate into a considerably larger retweet number value in support of a person, policy or narrative of significance (Wilson, 2011). Thus the ability for an association to dominate a larger than deserved share of the Twitter traffic, (along with its associated influence), is entirely possible using a set of malfeasant tactics. The Iranian government elections of 2009 experienced extensive bouts of slacktivism, where Twitter followers mistook a proliferation of invented blog feeds and botnets for authentic discrete political narratives (Christensen, 2011). In two-party dominated elections such as those in the United States and in Australia, where prominence is sited on the support for one political leader over another, party machines can enlarge the impact of their message using sock puppetry to augment the perception of support. During the 2013 federal elections in Australia, both the incumbent Prime Minister and the Leader of the Opposition were attributed with overly large numbers of fake Twitter followers (Butt & Hounslow, 2013).

Meat-puppets and Botnets: retweets for hire.

Sock-puppetry's nastier extension is 'meat-puppetry' where much larger quantities of on-line followers can be 'activated'. Typically a paid-for group intentionally lends its Twitter support for a particular person or narrative promotion. Such mass followings for hire are comprised of phony Twitter accounts that fall under the control of a single entity that sells their allegiance for a price (Ashton, 2013). Kevin Ashton's imaginary motivational speaker 'Santiago Swallow' was legendarily raised up in prominence through the purchase of 90,000 fake followers for the sum of US$50. Ashton created the fake account in less than 2 hours, searched the website fiverr.com for publics selling Twitter followers, and generated Santiago Swallow on the 13th of April 2013. He was then able to acquire reports from dependable social media analysts such as PeopleBrowsr, who announced that Santiago Swallow had an @Kred (2013) influence score of 754 out of 1000 (Ashton, 2013, Butt & Hounslow 2013).

Social networks, especially Twitter, are renowned for spreading misinformation and propaganda where web-based botnets command a considerable portion of twitter traffic (Boshmaf, Muslukhov, Beznosov and Ripeanu, 2011). Botnets form an unethical but significant segment of the twitter community (Chen, 2010). On the one hand, botnets are a necessary and legitimate component of the online information business market. On the other hand, they are tools that are used to deceive and manipulate the passage, transfer, and volume of social narrative. Ashton's Twitter creation was actuated using a trial copy of TweetAdder, that deployed a simple application to automatically dispense 'Santiago Swallow's tweets at regular intervals (McGee, 2013; Ashton, 2013). This automated program rapidly established a pattern of Twitter interaction, and copied popular comments from other online postings in order to establish an identity that seemed broad-minded, progressive and trendy.

Depicting fakes from real users and the need for Multi-Factor authentication

Although there is considerable substantiation of sock puppetry within the wider Twitter community (Krebs, 2011; Wheatley, 2013), it is especially noticeable during election phases, where the allegiance for a political leader may influence the perceptions and decisions of a much larger cohort of voters (Parmelee & Bichard, 2013). Ascertaining the difference between fake tweets and genuine tweets takes on a greater level of importance. In social and political terms (assuming prominent leaders have not been denied access to their own Twitter accounts) the measure of influence is best understood in terms of the proportion, direction, and frequency of the retweeted narrative (Parmelee & Bichard, 2013). A useful method was developed by Chu (et al., 2010) that determined whether retweets were created by humans, bots or cyborgs by partitioning retweeting humans as genuine followers who subscribe to the original authorship of others.

Unlike many web-based platforms, Twitter does not repeatedly challenge the identity of retweeting entities to question whether a bot-like entity is at work. Twitter simply asks for a CAPTCHA image during the registration and set up of a Twitter account. Consequently, once the login has been completed, bots can perform the majority of human twitter activities by calling on Twitter APIs. Creating and deploying a twitter-bot is a perfunctory exercise. Once started, a Twitter-bot relays the narrative of others as per its coded direction. After its initiation, the bot-like qualities of a twitter bot make it relatively easy to depict from the more random qualities that are attributed to genuine and discrete human users. Sitting between humans and bots there is a third group which Chu (et al., 2010) refers to as cyborgs. These Twitter entities are part-human and part-bot (Edwards, Edwards, Spence and Shelton, 2013). In some examples they are human-assisted bots and in other cases they are bot-assisted humans. One example might be as follows: a human Twitter subscriber logs in and sets up a number of automated feeder programs such as RSS feeds and Blog widgets. The Twitter entity then retweets a number of messages showing regular activity. The subscriber then also revisits his cyborg entity in an ad hoc manner and further enhances its 'humanness' by posting intermittent narrative to interact with other 'known' friends. The resultant Twitter traffic looks decidedly human, even though the great majority of the traffic is automated.

The authentication of identity on social media is paramount to the notion of trust. The speed of delivery and diffusion in Twitter means that influence can be gained quickly as followers retweet and observe the passage and support for narratives in real-time. Added metadata such as hashtags, attached pictures and URLs (as typically gathered by twitter-bots) adds to the perception of authority and information reliability (Cha, Haddadi, Benevenuto, & Gummadi, 2010). Thus the behavior of bot-nets and cyborgs within Twitter augments the perception of homophily which creates false bonding between followers and wider Twitter audiences (Nusselder, 2013). The introduction of multi-factor authentication in Twitter is an important step in reducing the number of fake retweets (Libicki, Balkovich, Jackson, Rudavsky & Webb, 2011).

The delineation of bots and cyborgs from authentic Twitter entities can be undertaken by looking at a small range of criteria. Chu et al (2010) proposed a four way test to differentiate Twitter phonies from humans. In the first instance, measuring the time intervals between retweets can reliably detect automated messaging. Scanning for signs of spam was also consistent since humans seldom deliberately send spam, as was examining the account properties of each subscriber, since those subscribers with no real account details, pictures, or descriptors, rarely indicated discrete personages. Moreover, bots are far more likely to post URLs than humans. An examination of these variables in concert therefore, assisted to establish the authenticity of retweeting followers (Chu, et al., 2010).

	Four Way Test for Twitter entities.
1.	*Entropy Test - Measure Retweet intervals*
2.	*Spam and Miscreant Test - Check for Benign or Malicious content*
3.	*Account Properties – Does the Account have subscriber details or does it look hollow*
4.	*Discrimination Analysis – combining Entropy, Spam, and Account Properties to evaluate all three indicators*

Table 1. Chu et al. (2010) 4 way test to distinguish humans from bots and cyborgs

Political Twitter Deception

Large scale meat-puppetry in Twitter represents a plausible method for increasing political participation (Hamdy, 2010; Wilson, 2011; Parmelee & Bichard, 2013). There is a close association with augmented retweets in political elections that suggests the presence of wide-spread sock puppetry (Stieglitz and Dang-Xuan, 2012). Sock puppetry in Twitter retweets is strengthened by the use of metadata, specifically URLs and #hashtags (Suh, Lichan, Pirolli, & Chi, 2010; Yang & Counts, 2010). Retweets often contains policy-event '#hashtags', to gauge the acceptance or significance of actions, policies, or individuals. Thus in political Twitter communities, where a specific event such as an election is in play, the retweet components allow for the amplification of political narratives through sock puppetry.

The elevation from sock puppetry to meat-puppetry represents the difference between subscribers with a handful of fake personas to the business of summoning thousands of automated fake followers who are paid for, arranged, and predisposed to retweet upon command (Wheatley, 2013). Meat puppets are fundamentally 'guns for hire' that can be activated at a moment's notice. The Russian election in 2011 exemplified the meat-puppetry of fraudsters who harnessed 25000 Twitter accounts in order to send 440,000 retweeted messages. Consequently normal discourse of election-based narrative and counter narrative was severely disrupted and interfered with (Thomas, Grier, and Paxson, 2012). Further inquiry exposed a *spam as a service* botnet that controlled over 975,000 Twitter accounts and mail.Ru email addresses (Thomas et al, 2012; Krebs, 2011). Most of the IP addresses connected with the disruption originated from beyond Russia, indicating the global agility with which sock puppetry influences domestic politics (Krebs, 2011).

Businesses proffering meat-puppets are open about the services that they offer. The British firm Buy More Followers publicizes a variety of new media products with scalable packages of up to 100,000 followers who have the appearance of authenticity (Evon, 2013). Other online entities that trade in increased automated Twitter followings and *spam-as-a-service* retweets include Fast Followerz, Deyumi, and FollowerSale (TwitterTop, 2013). Global traders such as these offer a range of influence services that extend beyond Twitter retweets into spamming, phishing, and infiltrating the overall balance of Twitter traffic (Wheatley, 2013). The effect of sock puppetry on this level indicates the attraction of purchasing support to sway the perceptions and interpretations of Twitter users to influence the outcomes of national and international elections.

Case Study into the Retweet data during the 2013 Australian Federal Election.

The 2013 Australian federal election experienced mixed reaction to the retweet activity that followed the two main party leaders vying for the position of Prime Minister. Candidates Tony Abbott and Kevin Rudd both had significant followings on Twitter. Using Abbott and Rudd's leadership tweets, this case study scrutinized 30,535 first generation retweets with a total of 10,201 retweets from Abbott tweets and 20,334 retweets from Rudd tweets. Under similar electoral conditions Chu et al., (2010) and Wilson (2011) predicted significant influence from fake retweets, bots and cyborgs. With the election on the 7th of September 2013, the Twitter activity in the immediate pre- and post- election weeks allowed for an analysis of retweeter behavior. This study hypothesized that it is conceivable to differentiate fake and automated retweets by comparing retweets with key election days that spawned high-interest policy statements, as well as examining follower inactivity before the election, and after the election. A second hypothesis posited that slacktivism guides the Twitter behavior of politically vested followers. This hypothesis looks to demonstrate the emergence of 'social - loafing' where followers will retweet political and election narrative without regard for author identity, authenticity or narrative information. The study aimed to show larger than normal numbers of Twitter followers, botnets, sock puppets, and their associated retweets in support of political leaders.

Methodology

With the intention of examining online fake electoral personas in Australia, the Twitter accounts (*@TonyAbbottMHR* and *@KRuddMP*) of the two main candidates for Australian Prime Minister were used as launch points to measure the associated followers, and their retweeting activities. The samples were collected from open source content, available by following the accounts through Twitter.com. Building on Chu's (et al., 2010) original test using four criteria, a nine-way test was derived that included the original four of Chu's variables, with additional markers for specific event and date-based activity (*Table 2*.). The test also looked for accounts which were characterized by 'exclusively single generation' retweet behavior, on the basis that bots don't retweet other bots.

	Nine Way Test for Twitter entities in an Election.

1.	*Entropy Test - Measure Retweet intervals*
2.	*Spam and Miscreant Test - Check for Benign or Malicious content*
3.	*Account Properties – Does the Account have subscriber details or does it look hollow*
4.	*Accounts Created on or about August the 4th 2013. (Announcement of Election)*
5.	*Inactivity before the election*
6.	*Inactivity after the election*
7.	*Follower alignments – Bots don't follow other Bots*
8.	*Mass retweets on policy-specific days and times*
9.	*Discrimination Analysis – combining Entropy, Spam, and Account, Inactivity, Alignments, and Mass retweets.*

Table 2. A nine-way test to distinguish fake retweets in the 2013 Federal Election (adapted from Chu et al, 2010)

Analysis of Results

The key variables showed large numbers of probable bots based upon their retweet intervals. Humans tend to retweet at different times of the day, and in different ways. Bots that are automated to retweet will send narratives at very exacting intervals (eg every 4 hours, or at exactly the same time each day). The increased presence of spam showed probable botnets, since humans rarely retweet spam. In combination, the presence of bots increases exponentially, since humans rarely retweet spam, and if they did, they would be extremely unlikely to retweet that spam at the exact same time each day. Account details are also useful markers. Accounts that show few details, no pictures, and with default background settings are more likely to be bots. Again, in combination with the other variables, the likelihood of certain followers being fake bots increases appreciably.

Other 'date-specific' variables offer even more divergence from human followers. Twitter accounts that were activated either on, or just after, the announcement of the federal election date show higher probability of being botnets. Similarly, large numbers of followers of both Tony Abbott and Kevin Rudd showed almost complete inactivity before the election announcement, and after the election result was announced. Those retweets that showed similar followings with each other, shared a positive relationship with other botnet characteristics, but never retweeted each other, look remarkably automated. Bots don't retweet other bots. Key policy dates also showed strong co-variation between increased retweets and the combined nine-way test variables. Throughout the data sample there existed strong rationale and reasonable explanation suggesting the deployment of bots.

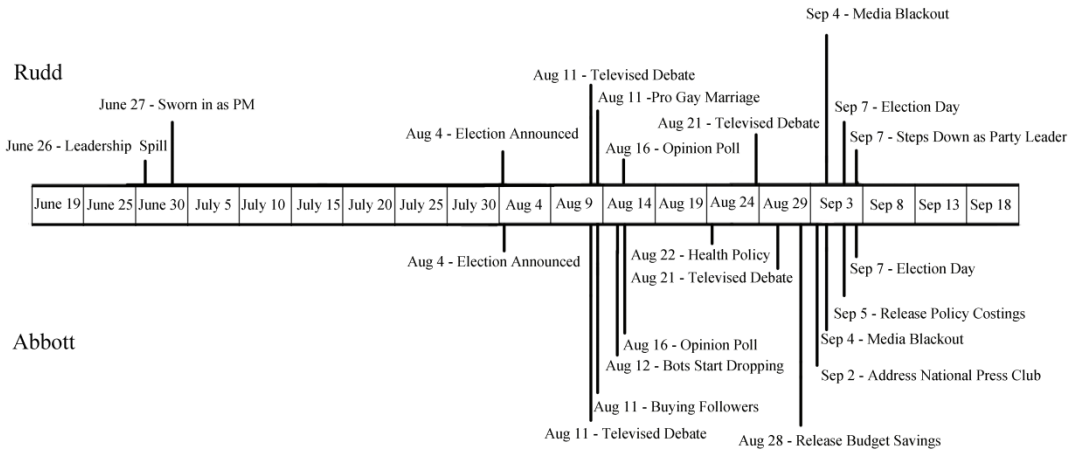

Figure 1. Key Dates in the 2013 Australian federal Election.

Specific dates also revealed the likely presence of botnets. As previously discussed, large numbers of followers started retweeting after the 4th of August (the announcement of the election date). These included Twitter accounts that had lain dormant for many months, or whose creation occurred on or just after the 4th of August.

On August the 11th the numbers of followers for Tony Abbott increased dramatically, suggesting the acquisition of bots on a meat-puppet scale. Abbott's followers went from 165,235 to total of 234,167 followers, a rise of 68932 within 48 hours (Ralston, 2013). After media conjecture that Abbott had acquired the services of meat-puppets, the numbers dropped by 43,357 followers within the following 24 hour period (Ralston, 2013). The same characteristic aligned positively with Rudd's Twitter followers. Again, on the 12th of September more than 50000 followers of Kevin Rudd suddenly dropped off the list of Rudd followers after media speculation that the Twitter accounts had been 'hired" as a force multiplier to portray support for Kevin Rudd's election campaign (Andrews, 2013). Whilst it is possible that more than 100000 individual Twitter followers joined up to Rudd and Abbott with 24 hours, in combination with media speculation and the subsequent mass dumping of Twitter accounts, the more likely proposition is that these Twitter accounts were fake, and have been acquired (and released) *en mass*.

The impact of fake Twitter accounts is disguised amongst the combined traffic of genuine human accounts and fake Twitter multipliers. The analysis showed an amalgamation of paid-for botnets, and party-aligned cyborgs (party faithful users with multiple Twitter accounts). The paid-for botnets showed strong positive grouping with each other, often behaving in exactly the same manner, and retweeting exactly the same narratives, and where possible, the same overt metatagging of a URL within the 140 characters of the Twitter message. These retweets show as automatic feeds that are re-expressed so as to imitate individual messages of party support with the aggregated influence of large numbers of retweets. Typical groupings of these retweets present in groups of several thousand at a time, with retweeted messages deploying at regular (robotic) intervals. The cyborg retweets were more difficult to detect, since although they displayed many of the same automated response characteristics of the large group meat-puppets, would also show occasional personalized messages. These personalized messages reinforced the idea that Twitter accounts were real individuals, when infact they were multiplied expressions of a handful of users. Cyborgs present in smaller groupings, typically from 5-15 expressions. Some of their 'personalised' messages were identical to the 'personalised' messages of other fellow cyborgs, simply messaged at different (although automated) intervals.

Limitations on botnets and cyborgs

Although very large numbers of retweets display the obvious characteristics of automation and the presence of fake personas, there is also the reverse possibility of some humans behaving as bots (Gianvecchio, Xie, Wu and Wang, 2008). One of the inherent attractions of Twitter (more than other social media platforms) is the ability to simply copy and retweet someone else's narrative (Edwards et al., 2013). Therefore whilst unlikely, we cannot discount the possibility that some genuine persons may have behaved in a robotic manner so as to look like bot nets within this study. Twitter allows for otherwise shy people to engage in an information exchange that builds on the repetition of someone else's message (Celli, 2011; Zhao and Rosson, 2009). Additionally politics can be a confronting topic to engage with individually and socially (Morozov, 2009). There is a small percentage of the data that has been aggregated as either botnets or cyborgs who are quite possibly human (Edwards et al., 2013).

Slacktivism in Political Retweets

There is conjecture about the validity of the support that flows from retweeted political narrative (Christensen, 2011). Slacktivists are deemed as social active yet either ignorant, naïve or lazy towards large samples of non-genuine twitter support. They mistakenly confuse auto-narrative for genuinely supported political posturing. Whilst the media has covered many high profile examples of Twitter deception, the on-line public has remained relatively silent. In the case of the Australian federal election, there would be cause for concern if micro-blogging were seen to deceive the public. Section 329 of the Australian Commonwealth Electoral Act of 1918 states:

Misleading or deceptive publications:

> *"A person shall not, during the relevant period in relation to an election under this Act, print, publish or distribute, or cause, permit or authorize to be printed, published or distributed, any matter or thing that is likely to mislead or deceive an elector in relation to the casting of a vote."* (Commonwealth Electoral Act, 1918).

The question arises as to whether any electors in the 2013 Australian federal election were sufficiently influenced by the retweeted support or multiplied narrative in terms of their voting behavior. Do retweets constitute 'published material'? If botnets and cyborg-generated spam represents misleading electoral advertising (by virtue of its existence through fake personas), then there is reason to examine the legal means of

distinguishing between real retweets and those from their fake, multiple identities (AEC, 2013). If we assume that botnets are widespread in the same way that tweets are ubiquitous, then we could assume that any and all retweets should be treated as unverified. However, if the retweets of political election narrative were treated in the same way that political messages on printed posters are considered, then the Australian Electoral Commission would need to take action (AEC, 2013). Instead, this paper assumes that slacktivism drives public acceptance of retweeted micro-blogging regardless of frequency or pervasiveness.

The issue of fake retweets is globally significant (Wilson 2011; Stieglitz & Dang-Xuan, 2012). In an American context, slacktivism should be of greater concern where there is already discontent from individuals who feel restricted by the Federal election Campaign Act (FECA) laws that limit the amount of electoral donations to candidates (FEC, 2013). In the United Kingdom, the Director of Public Prosecutions stated that "communications that are merely indecent, obscene or false will be prosecuted only when it can be shown to be necessary and proportionate" (CBS, 2012). Since the cost of meat-puppetry is both inexpensive (Ashton, 2013) and largely untraceable (Krebs, 2011), it begs the question as to whether fake twitter accounts represent an overly significant percentage of twitter traffic in attempts at fair and democratic elections.

Hypotheses 1 and 2 Results

The first hypothesis asked whether it was possible to distinguish fake, automated retweets from human ones. The nine-way test revealed more than 28000 followers (combines Rudd and Abbott data) that aligned with the combined features of entropy, spam, identity hollowness, automated retweet intervals, and pre or post retweet inactivity. A combination of Twitter botnets and cyborgs, in the form of both sockpuppets and meat-puppets, interacted regularly with the postings of either the @TonyAbbottMHR or the @KRuddMP Twitter accounts from the period of the 4th of August through until the 18th of September in 2013. The second theory builds upon the positive results of the first hypothesis. Since the detection of large numbers of automated retweets from fake personas operating Twitter accounts was openly discussed in mainstream media, yet not debated beyond initial reporting, a reasonable conclusion is that political parties not only tolerate slacktivism, they accept the benefit of 'slacker activists' whether in human, botnet or cyborg form.

CONCLUSION

The 2013 Australian federal elections encountered many thousands of automated, non-genuine, fake Twitter entities that retweeted political narratives in support of the two opposing political leaders Kevin Rudd and Tony Abbott. These entities included a consolidation of botnets, cyborgs, sock-puppets and meat-puppets. Their existence as such a striking statistic denotes that retweeted narratives are not a reliable measurement for depicting the impact and influence of political issues and their online discourse. The absence of strong response and public outcry to obvious sock puppetry and its subsequent withdrawal, implies that slacktivism is becoming an accepted element in new media. Whichever electoral campaign that rationales support for an issue or candidate on the basis of Twitter retweets should renounce the significant distortion that fake personas displace into the political landscape.

AUTHORS NOTES:

Some elements of this study were previously presented at the 14th Australian Information Warfare and Security Conference in the Edith Cowan University Security Research Institute (2nd - 4th December 2013), Perth, Western Australia.

REFERENCES

@Kred. (2013) Kred Social Media Influence Platform, retrieved from Twitter on the 23rd September 2013 at: https://twitter.com/Kred

AEC. (2013). Electoral Offences, Australian Electoral Commission, Election 2013, retrieved October 14th from: http://www.aec.gov.au/elections/australian_electoral_system/electoral_procedures/Electoral_Offences.htm

Andrews, T. (2013) Kevin Rudd buying twitter followers to boost Leadership Bid, *Menzies House*, Retrieved 3rd October from: http://www.menzieshouse.com.au/2011/09/exclusive-investigation-kevin-rudd-buying-twitter-followers-to-boost-leadership-bid.html

Ashton, K. (2013) Tweeto Ergo Sum: How to become internet famous for $68. *Quartz*, retrieved 29th September 2013 from http://qz.com/74937/how-to-become-internet-famous-without-ever-existing/

Bartlett, J., Birdwell, J., & Littler, M. (2011). *The new face of digital populism*. Demos 7, 2011.

Boshmaf, Y., Muslukhov, I., Beznosov, K., and Ripeanu, M. (2011). The socialbot network: when bots socialize for fame and money. Proceedings of the *27th Annual Computer security Applications Conference*, ACM, New York, pp93 – 102.

Butt, C., & Hounslow, T. (2013) Fake followers boost politicians' Twitter popularity, *The Sydney Morning Herald*,: Datapoint, retrieved 24th September 2013 from: http://www.smh.com.au/data-point/fake-followers-boost-politicians-twitter-popularity-20130427-2ilmm.html

Cao, Q., Sirivianos, M., Yang, X., & Pregueiro, T. (2012) Aiding the Detection of Fake Accounts in large Scale Online Services, *Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation* (NSDI) April 25 – 27, 2012.

CBS. (2012). "U.K. sets out social media prosecution guidelines" CBS News (Associated Press), 19th December 2012, Retrieved 4th October from: http://www.cbsnews.com/news/uk-sets-out-social-media-prosecution-guidelines/

Celli, F. (2011). Mining User Personality in Twitter, *Language, Interaction and Computation CLIC*, University of Trento, retrieved 4th October 2013 from: http://clic.cimec.unitn.it/

Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, K. (2010). Measuring User Influence in Twitter: The Million Follower Fallacy, *Proceedings of the 4th International AAAI Conference on Weblogs and Social Media*, May 23-26, 2010, George Washington University, Washington DC., retrieved 13th October 2010 from: http://snap.stanford.edu/class/cs224w-readings/cha10influence.pdf

Chen, S. (2010) Self-Governing Online Communities in Web 2.0: Privacy, Anonimity and Accountability. *Albany Law Journal of Science and Technology.*

Christensen, C. (2011). Twitter Revolutions? Addressing Social Media and Dissent, *The Communication Review*, Volume 14, Issue 3, **DOI:**10.1080/10714421.2011.597235.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010). Who is tweeting on Twitter: Human, Bot, or Cyborg? in the *Proceedings of the 26th Annual Computer Security Applications Conference,* ACSAC '10, pp21-30.

Cogburn & Espinoza-Vasquez, (2011). From networked nominee to networked nation: Examining the impact of web 2.0 and social media on political participation and civic engagement in the 2008 Obama campaign. *Journal of Political Marketing.* Volume 10, pp 189-213.

Commonwealth Electoral Act, (1918). Commonwealth Electoral Act 1918 – Section 329, Misleading or deceptive publications etc. Commonwealth Consolidated Acts, retrieved 14th October 2013 from: http://www.austlii.edu.au/au/legis/cth/consol_act/cea1918233/s329.html

Conway, M. (2012). *From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu. Retrieved from http://www.isodarco.it/*

D'Yonfro, J. (2013) Twitter Admits 5% of its 'users' are Fake. *Business Insider Australia*, Retrieved October 13th from: http://www.businessinsider.com.au/5-of-twitter-monthly-active-users-are-fake-2013-10

Edwards, C., Edwards, A., Spence, P.R., and Shelton, A.K. (2013) Is that a bot running the social media feed? Testing the differences in perceptions of communications quality for a human agent and a bot agent on Twitter, *Computers in Human Behaviour*, Volume 31, http://www.sciencedirect.com/science/journal/07475632/30

Evon, D. (2013). Get More Twitter Followers: What Buying Fake Followers will (and will not) do for you, Social News Daily, retrieved October 4th 2013 from: http://socialnewsdaily.com/17305/get-twitter-followers-buying-fake-followers-will-will/

FEC, (2013). Federal Election Commission, Laws & Regulations, Federal Election Campaign Act; retrieved December 28th 2013 from: http://www.fec.gov/law/law.shtml

Gianvecchio, S., Xie, M., Wu, Z., and Wang, H. (2008) Measurement and Classification of Humans and Bots in Internet Chat, USENIX Security Symposium, 2008, retrieved 23rd September 2013 from https://www.usenix.org/legacy/event/sec08/tech/full_papers/gianvecchio/gianvecchio_html/

Gleason, B. (2013). Movement on Twitter #Occupy Wall Street: Exploring Informal Learning About a Social Movement on Twitter. *American Behavioural Scientist, 57(7), 966-982.*

Hamdy, N. (2010). Arab media adopt citizen journalism to change the dynamics of conflict coverage. *Global Media Journal:* Arabian Edition*,* **1***(*1*),* 3–15

Howard, (2011). *The digital origins of dictatorship and democracy: Information technology and political Islam.* London, UK: Oxford University Press. *DOI: 10.1093/acprof:oso/ 9780199736416.003.0004*

Jansen, B. J.*,* Zhang, M.*,* Sobel, K.*, &* Chowdury, A. *(*2009*).* Twitter power: Tweets as electronic word of mouth. *Journal of the American Society for Information Science and Technology,* **60***(*11*),* 2169–2188. DOI: 10.1002/asi.21149

Jeffries, S. (2010). A rare interview with Jurgen Habermas, *The Financial Times*, retrieved September 29th 2013 from:http://www.zunehmender-grenznutzen.de/wpcontent/uploads/2010/05/Habermas_Greece_Financial_Crisis.pdf

Jewitt, R., (2009). Commentaries: The trouble with twittering: Integrating social media into mainstream news. *International Journal of Media and Cultural Politics,* **5***(*3*),* 233–246. DOI: 10.1386/macp.5.3.233/3

Krebs, B. (2011). Twitter Bots Drown out Anti-Kremlin Tweets, *Krebs on Security*: In-depth security news and investigation, Retrieved October 14th 2013 from: https://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/

Kwak Lee, C.*,* Park, H.*, &* Moon, S. *(*2010*). What is Twitter: A social network or a news media.* Proceedings of the 19 th International Conference on the World Wide Web (pp. *591–600*). New York, NY: ACM.

Libicki, M. C., Balkovich, E., Jackson, B.A., Rudavsky, R., & Webb, K.W. (2011). Influences on the Adoption of Multifactor Authentication, Technical Report, RAND Homeland Security and Defense Center, Retrieved 10th September from: http://www.rand.org/pubs/technical_reports/TR937.html

Lloyd, G. (2012). *The Social Pandemic; The Influence and Effect of Social Media on Modern Life*. Leicester, England: CreateSpace Independent.

McGee, M. (2013). Twitter Reaches Spam Lawsuit settlement with Tweet Adder, *Marketing Land*, retrieved on the 30th October 2013 from: http://marketingland.com/twitter-reaches-spam-lawsuit-settlement-with-tweet-adder-45890

Morozov, E. (2009) From Slacktivism to Activism, in *Foreign Policy: Net.Effect*, *How Technology shapes the World,* first posted on Saturday September the 5th, 2009. Article retrieved 6th October 2013 from: http://neteffect.foreignpolicy.com/posts/2009/09/05/from_slacktivism_to_activism?wp_login_redirect=0

Nusselder, A. (2013). Twitter and the personalization of politics, *Journal of Psychoanalysis, Culture and Society*, Volume 19=8, pp91 – 100, DOI: 10.1057/pcs.2012.45

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age.* Cambridge, England: Polity Press.

Papacharissi, Z., and Oliviera, M., (2012) Affective News and Networked Publics: The Rhythms of News Storytelling on #Egypt, *Journal of Communication*, Volume 62, Issue 2, pp266-282.

Parmelee, J. H. & Bichard, S. L. (2013). *Politics and the Twitter Revolution.* Lanham, Maryland: Lexington Books.

Ralston, N. (2013). Tony Abbott's Twitter followers drops after fake buyers culled, *Sydney Morning Herald*, SMH, Retreived 4th October from http://www.smh.com.au/federal-politics/federal-election-2013/tony-abbotts-twitter-followers-drops-after-fake-buyers-culled-20130811-2rpt2.html

Rollins, D. (1993) Arty/Scotto bit list server Dana Rollins, retrieved 4th October 2013 from: https://groups.google.com/forum/#!msg/bit.listserv.fnord-l/D_wlg9YXFA0/n0aWLZwctdEJ

Solow-Niederman, A. G. (2010) The power of 140 characters? #IranElection and social movements in web 2.0. *Intersect*, **3***(*1*),* 30–39

Stieglitz, S., & Dang-Xuan, L. (2012). Political Communication and Influence through Microblogging – An Empirical Analysis of Sentiment in Twitter Messages and Retweet Behaviour, Proceedings of the 45th Hawaii International Conference on System Sciences, (HICSS), retrieved on the 4th of October 2013 from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6149247

Streitfield, D. (2012). The best Book Reviews money Can Buy, *The New York Times*, retrieved October 1st 2013 from http://www.nytimes.com/2012/08/26/business/book-reviewers-for-hire-meet-a-demand-for-online-raves.html?_r=5&pagewanted=all&

Suh, B., Lichan, H., Pirolli, P., & Chi, E.H. (2010). *Want to be Retweeted? Large Scale Analytics on Factors Impacting Retweet in Twitter Network.* 2010 IEEE 2nd International Conference on Social Computing.

Thomas, K., Grier, C., & Paxson, V. (2012). Adapting Social Spam Infrastructure for Political Censorship, *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats*. San Jose, California.

Twitter. (2013). *Twitter; An Information Network*, retrieved 25th September 2013 from: https://twitter.com/about

TwitterTop. (2013) Best Websites to Gain Free Twitter Followers. Retrieved October 14th 2013 from: http://twittertop.com/

United States Securities and Exchange Commission, (2013). Form S-1 Twitter Inc. Registration No. 333, US Securities and Exchange Commission, Washington D.C. 20549, Retrieved October 17th from: http://www.sec.gov/Archives/edgar/data/1418091/000119312513390321/d564001ds1.htm

Waters, R. D., & Williams, J. M. (2011) Squawking, Tweeting, Cooing, and Hooting: analyzing the communication patterns of government agencies on Twitter, *Journal of Public Affairs*, Volume 11, No 4 pp 353-363 DOI: 10.1002/pa.385

Wheatley, M. (2013). Twitter Shoots down TweetAdder in War on Spam, *Silicon Angle*, retrieved 14th October 2013 from: http://siliconangle.com/blog/2013/05/29/twitter-shoots-down-tweetadder-in-war-on-spam/

Wilson, J. (2011). Playing with Politics: Political Fans and Twitter faking in post-broadcast democracy, *Convergence: The International Journal of Research into New Media technologies*. DOI: 10.1177//1354856511414348

Yang, J., and Counts, S. (2010). *Predicting the Speed, Scale and Range of Information Diffusion in Twitter*, Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, George Washington University May 23-26th, 2010.

Yarow, J. (2013) Twitter's IPO Filing is Out, *Business Insider Australia,* Retrieved October 13th from: http://www.businessinsider.com.au/twitter-ipo-filing-2013-10

Zhao, D., & Rosson, M. B. (2009). How and why people Twitter: The role that micro blogging plays in informal communication at work, Proceedings of GROUP, ACM, pp243 – 252, New York 2009.

Zhang, Y., Hong, J., & Cranor, L. (2007) CANTINA: A Content-Based Approach to detecting Phishing Web Sites. *Proceedings of the 16th International Conference on the World Wide Web,* pp 639 – 648, Retrieved 31st October 2013 from http://dl.acm.org/citation.cfm?id=1242659