Aston University

Centre for Forensic Linguistics

**The First Annual Centre for Forensic Linguistics (CFL) Symposium**
**Cybercrime: Language and Identities Online**

Friday 20th May 2016
Conference Aston Conference Centre & Hotel (Aston Business School),
Aston Triangle, Birmingham, B4 7ET

**Programme**

| | |
|---|---|
| **09.00-09.30** | REGISTRATION AND COFFEE (Courtyard Lounge) |
| **09.30-09.45** | Welcome (Room 123, 1st Floor) |
| **09.45-10.45** | Keynote 1: Professor Tim Grant and Dr Nicci MacLeod (CFL, Aston University, UK)<br>*Assuming identities online: Moving from individual criminals to criminal communities of practice* |
| **10.45 – 11.15** | TEA BREAK (Courtyard Lounge) |
| **11.15-11.45** | Emily Carmody (CFL, Aston University, UK)<br>*Move maps: A move analysis of chatroom grooming interactions* |
| **11.45-12.15** | Annie Houle (Université du Québec à Trois-Rivières, Canada)<br>*Dismissing suspicion about identity or how to fix a cracked frame* |
| **12.15-12.45** | Dr Ria Perkins (CFL, Aston University, UK)<br>*Share if you agree: the linguistic features and persuasive elements of viral messaging* |
| **12.45-13.15** | Olumide Popoola (CFL, Aston University, UK)<br>*Understanding the discourse of deception: deception strategies for fake online reviews* |
| **13.15-14.15** | LUNCH (Courtyard Restaurant) |
| **14.15-15.15** | Keynote 2: Dr Claire Hardaker (Lancaster University, UK)<br>*Finding Ashley's Angels: identifying Ashley Madison Angel profiles using forensic/corpus linguistics* |
| **15.15-15.45** | Dr Alison Johnson (University of Leeds, UK) & Dr David Wright (Nottingham Trent University, UK)<br>*Business-only or business and pleasure identities? Constructing styles and stances in online email interaction* |
| **15.45-16.15** | Dr Rui Sousa Silva (Universidade do Porto, Portugal)<br>*'A Wink's Not as Good as a Nod': a new paradigm for forensic authorship analysis?* |
| **16.15-16.45** | Colin Michell (Fujairah Men's College, United Arab Emirates)<br>*Comparing the language used by the same person on two separate online platforms (blogs and Twitter)* |
| **16.45-17.00** | TEA BREAK (Courtyard Lounge) |
| **17.00 – 17.30** | Plenary discussion led by Prof. Tim Grant |

## Abstracts

### Keynote I

**Professor Tim Grant & Dr Nicci MacLeod (CFL, Aston University, UK)**

*Assuming Identities Online: Moving from individual criminals to criminal communities of practice*

The issue of identity and influence within online communities has become a significant security concern. Specifically with the rise of generally available hard encryption, the investigation of online communications increasingly poses its own unique set of challenges for investigators of paedophilia, terrorism, organised crime and other threats to the safety and security of groups and individuals.

This paper reports on a 2-year ESRC- funded project – Assuming Identities Online (AIO), which began in August 2014. The project aims to examine the relationship between language and online identity performance and address the question of what linguistic analysis is necessary and sufficient to describe an online linguistic persona to the extent it could be successfully assumed by another individual. To this end, a series of experiments was designed in which participants engaged with each other over Instant Messaging (IM), before an impersonation situation was engineered. Information was collected about what level of accuracy and confidence individuals can detect the substitution of one interlocutor with another, what linguistic criteria give rise to such suspicions, and how individuals prepare for impersonation tasks. The data generated by these experiments are drawn on in this paper, along with other data sets including from police training and operational settings where identity disguise is employed online in the context of investigations into child grooming and paedophilic image sharing. In a departure from both traditional sociolinguistics *and* the vast majority of scholarly work in the area of automated and semi-automated authorship analysis (e.g. Argamon *et al.,* 2003; Schler *et al.* 2006), we do not simplistically treat identity as a static collection of categories to which an individual either does or does not belong, but as a fluid, emergent, co-constructed and at least partially conscious process of performance. From our perspective, it is imperative to understand identity as the *product* rather than the *source* of linguistic and other semiotic practices.

We demonstrate one of the key outcomes of the project – a software tool that allows for the semi-automation of the analysis of online identities, that we have been trialling for use in the area of undercover online investigations. Lastly, we discuss our planned development of the work, from the examination of the individual to that of online 'communities of practice' (Lave and Wenger, 1991), membership of which requires familiarity with group norms, including those surrounding communication (Eckert, 2006). In terms of the operational task this moves the project forward from exclusive attention on the imitation of an individual to the question of infiltration of a group.

*References*

Argamon, S., Koppel, M., Fine, J., & Shimoni, A. R. (2003). 'Gender, genre, and writing style in formal written texts'. *Text* 23 (3)

Eckert, P. (2006) Communities of Practice. *Encyclopedia of Language and Linguistics*, 2,. Amsterdam: Elsevier. Pp 683-685

Lave, J. and E. Wenger (1991). *Situated learning: Legitimate peripheral participation.* Cambridge, Cambridge University Press

Schler, J., Koppel, M., Argamon, S., & Pennebaker, J. (2006). 'Effects of age and gender on blogging'. *Proceedings of the AAAI Spring Symposia on Computational Approaches to Analyzing Weblogs*, 27–29

## Keynote II

**Dr Claire Hardaker (Lancaster University, UK)**

*Finding Ashley's Angels: identifying Ashley Madison Angel profiles using forensic/corpus linguistics*

Created in 2001 by Avid Life Media Inc., the Ashley Madison website describes itself as "the most famous name in infidelity and married dating" and uses the tagline "Life is short. Have an affair." In July 2015, an anonymous group calling itself the Impact Team contacted Avid Life Media, ordering them to take down Ashley Madison, as well as an associated site, Established Men. When Avid Life Media did not comply, over a series of days in August 2015, the Impact Team released onto the dark net several large data-dumps containing a wide array of information around thirty-two million users, including email addresses, geographical addresses, phone numbers, physical descriptions, personal habits, and sexual preferences. Within hours of this leak, it became apparent that not all the profiles on Ashley Madison were used by humans. Instead, some, known internally as Angels, were operated by software. Indeed, earlier iterations of the site's Terms & Conditions explicitly mentioned that some profiles were for "entertainment", but that these were "not conspicuously identified as such".

In this talk, I describe the results of an investigation into the Angel accounts and discuss ways we can establish their differences from ordinary accounts. To conduct the investigation, I used a newly developed freeware tool called FireAnt that made it possible to extract relevant profiles, visualise them spatiotemporally, and export the text from them for further forensic/corpus linguistic analyses. Overall, I address two research questions: (1) How many profiles in the leak are actually Angels? And (2) How convincing are those Angel profiles? i.e. Since a small number of people are typically trying to look like many unique individuals, how well are they doing at creating online identities that look like those of ordinary members?

**Emily Carmody (CFL, Aston University, UK)**
*Move maps: A move analysis of chatroom grooming interactions*

The sexual grooming of children through online communicative platforms is becoming an increasingly recognised problem. Most academic research in this area expectedly arises from psychology and criminology, but considering that online grooming occurs almost entirely through processes of written communication, linguistics has thus far offered comparatively little. The linguistic work that has been done has already contributed greatly to our understanding of online grooming practices (see O'Connell, 2003; Williams, Elliott & Beech, 2013; Black et al., 2015) and offered successful operational assistance in police training techniques (Grant & Macleod, 2016). The current research employs Swales' (1981) move analysis to examine transcripts of chatroom grooming interactions in terms of their broad discourse structures and the linguistic strategies involved in grooming. It considers some of the linguistic devices observed in the methods used by groomers to manage the risks associated with grooming children online, and proposes a method of visualising move structures in a way that allows the easy recognition and comparison of linguistic structures and patterns observed in chatroom grooming.

*References*

Black, P. J., Wollis, M., Woodworth, M. & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behaviour in an increasingly computer-mediated world. Child Abuse and Neglect, 44, 140-149.

Grant, T. and MacLeod, N. (2016). Assuming identities online: experimental linguistics applied to the policing of online paedophile activity. Applied linguistics 37, 1, 50-70.

O'Connell, R. (2003). A typology of cyber sexploitation and online grooming practices. Preston, England: Cyberspace Research Unit, University of Central Lancashire. [Online]. Available from: http://netsafe.org.nz/Doc_Library/racheloconnell1.pdf. [Accessed: 14th January 2015].

Swales, J. (1981). Aspects of Article Introductions: Aston ESP Research Reports No. 1. Language Studies Unit, Aston University, Birmingham.

Williams, R., Elliott, I. A. & Beech, A. R. (2013). Identifying Sexual Grooming Themes Used by Internet Sex Offenders. Deviant Behavior, 34(2), 135-152.

---

**Annie Houle (Université du Québec à Trois-Rivières, Canada)**
*Dismissing suspicion about identity or how to fix a cracked frame*

This study investigates the way voluntary undercover agents negotiate suspicion about their forged identity on the web. The data come from the website of Perverted-Justice, an American organization which gathers volunteers who pose as teenagers on the web to catch pedophile predators. Chat log archives leading to convictions by the help of their agents are available from www.perverted-justice.com. For the purpose of this study, we extracted every chat log archive that contains a sequence in which the predator asks overtly if his interlocutor is a police agent. Using a transversal conversation analysis approach, we examined these authentication sequences and observed that agents' reactions varied from direct negation to ironic affirmation. We also found that predators' evaluations of these answers are generally positive and short in terms of speech turns. Further contextual analysis helped us to identify, classify and evaluate linguistic strategies to dismiss suspicion according to the tone of the overall interaction, the tone of

the authentication sequence, the agent's answer, the predator's evaluation of this answer and the number of convictions made by the agent in question in each sequence.

---

**Dr Alison Johnson (University of Leeds, UK) and Dr David Wright (Nottingham Trent University, UK)**

*Business-only or business and pleasure identities? Constructing styles and stances in online email interaction*

Sociolinguistics research has, since the 1960s focused more on the language of the group – dialect, genderlect – than on the language of the individual: idiolect. Given that forensic linguistic research is, because of its professional interest in authorship attribution and the tracking of individuals online, more focused on idiolect, this paper attempts to draw the two together.

We focus on the Enron email corpus, a corpus of 176 authors in one company, which constitutes a 'community of practice' (Lave and Wenger 1991), a group of professionals sharing the same norms and practices and working towards shared goals.

Given that email is a hybrid genre, both a social, group-constructing activity and an individual endeavour, we ask: How do individuals construct their own unique identities within the social and professional groups and networks that make up a business? Do aspects of their professional and social identity overlap? We examine the language of 10 employees, 5 whose online email identity is constructed entirely on a professional basis and 5 who use email both for business and social purposes. In the 'business-only' group, we examine those features that users share and those which make them unique and in the 'business-and-pleasure group' in addition to analysing their business emails for shared and unique features, we investigate how variation and consistency are demonstrated across the business and pleasure modes.

Language acts are 'acts of identity' (Le Page and Tabouret-Keller 1985) and 'the sociolinguistic study of identity has increasingly become the study of style' (Bucholtz 2009: 146) in which speakers construct and display their identities and where 'the social meaning of linguistic forms' is subtly created in "interactional moves through which speakers take stances, create alignments, and construct personas' (Bucholtz 2009: 147). We therefore identify consistencies in these kinds of moves in both business and social style in online email interaction.

*References*

Bucholtz, M. 2009. From stance to style: Gender, interaction, and indexicality in Mexican immigrant youth slang. In A. Jaffe. Ed. *Stance: Sociolinguistic Perspectives.*Oxford: Oxford University Press, pp. 146-170.

Lave, J. & Wenger, E. 1991. *Situated Learning: Legitimate Peripheral Participation.* Cambridge: Cambridge University Press.

Le Page, R. B., & Tabouret-Keller, A. 1985. *Acts of identity: Creole-based approaches to language and ethnicity.* Cambridge: Cambridge University Press.

---

**Colin Michell** (**Fujairah Men's College, United Arab Emirates)**
*Comparing the language used by the same person on two separate online platforms (blogs and Twitter)*

An anonymous blog claiming that one of South Africa's best loved sports journalists is a fraud and a liar appeared in mid-2015. The journalist in question had been investigating corruption at the highest levels within the South African sporting administration and as a result was forced to flee South Africa to the safety of the United States. The authors of the defamatory blog have never identified themselves, and with a fake IP address in London and the server in Panama, it has been impossible to identify them, and shut down the blog.

Thankfully, sports journalism in South Africa is a fairly small industry, and the journalist in question had made a number of enemies over the years. This gave us a pool of potential suspects, but unfortunately none of them had any known blogs with which to compare language usage. All of them, however, do have active Twitter accounts, and they write regular columns in various sports magazines, and online forums. Even though Blogs and Twitter are slightly different genres of writing and have different constraints such as maximum number of words, enough of the features carried over to make comparisons.

My talk will focus on the stylistic similarities, such as multiple punctuation marks, and dissimilarities such as the use of hashtags of a single person's writing on two distinct online platforms. I will also look at how the chosen style markers compare in a stylometric analysis.

---

**Dr Ria Perkins (CFL, Aston University, UK)**
*Share if you agree: the linguistic features and persuasive elements of viral messaging*

Digital social media is playing an increasing role in the radicalisation of individuals, this paper analyses what linguistic elements make up successful viral messages. It focuses on the persuasive elements of viral messaging, and analyses how the linguistic features identified are employed to help a message 'go viral'. Findings are presented from a linguistic analysis of successful viral messages from social media. The research presented takes a data driven approach, with the viral messages that comprise the data being collected from a wide range of topics. The findings are then compared to comparable analysis of extremist and radicalising Twitter feeds.
This paper is grounded in a forensic linguistic perspective; it discusses the potential applications of a greater understanding of the persuasive linguistic features of viral messages, particularly with relation to understanding persuasive messages linked to terrorism or radicalisation. It also considers the potential benefits from a range of perspectives, including for law enforcement agencies. Due to the growing interest and concern surrounding online persuasion; especially relating to online radicalisation and grooming, this paper will analyse the findings with relation to the wider context of persuasion online. Despite the fact that language is integral to the persuasive process (Matustiz, 2013; McEnery, 2013) previous research into persuasion takes a predominantly marketing or psychological approach, with a limited focus on specific linguistic features. This current project is an initial step towards filling this gap, and has valuable applications in its own right.

*References*

McEnery, T. (2013). Primed for Violence? A corpus analysis of jihadist discourse. John Sinclair Lecture. Retrieved May 16, 2013, from http://www.birmingham.ac.uk/schools/edacs/departments/english/news/2013/tony-mcenery.aspx

Matusitz, J. (2013). Terrorism and Communication: A Critical Introduction. Los Angeles: SAGE Publications.

---

**Olumide Popoola (CFL, Aston University, UK)**

*Understanding the discourse of deception: deception strategies for fake online reviews*

54% of UK adults read online reviews before making a purchase (Competition and Markets Authority 2015). Although it is difficult to obtain exact figures, various research studies have calculated that 2-20% of online reviews are fake. With online sales contributing to over £20billion to the UK economy alone, deceptive online reviews are a billion pounds scam. Amazon's launch of legal action in the US against 1114 fake review sellers from a single website, indicates the global reach of the problem (Amazon.com. v. John Does 1-114).

So far, linguistic attempts to detect online opinion spam have preferred a range of lexicosemantic and syntactic techniques that either convert psycholinguistic tools (such as LIWC or Reality Monitoring) into equivalent computational features or utilize ngram-based text classification (e.g. Zhou et al., 2004; Yoo and Gretzel, 2009; Ott et al., 2011; Li et al., 2014; Anderson and Simester 2014). Whilst accuracy rates of 90% have been achieved on specific experimental datasets, these have results have not been replicable (see Fei et al., 2013). Furthermore, the linguistic deception cues identified do not show a uniform direction. All this points to the value of developing tools that look beyond bags of words and phrases to explore the discourse of deception.

This paper demonstrates how discourse analysis can improve deception detection by providing empirical linguistic evidence of the strategies deployed to create online reviews. Using Rhetorical Structure Theory (Mann and Thompson, 1988), a blind annotation of a sample of the DeRev corpus (Fornaciari and Poesio, 2012) of true and fake Amazon reviews was conducted by trained annotators to produce rhetorical prototypes of true and deceptive reviews. The resultant discourse profiles were then used to identify the veracity of the remaining Amazon reviews as well as a sample of genuine and paid hotel reviews from Tripadvisor.com.

This research shows the potential for discourse analysis to reconcile the contradictions found in lexicosemantic deception detection and provides a framework for the detection of opinion spam across genres and languages.

*References*

Amazon.com, Inc. v. John Does 1-114 , King County Case No. 15-2-25395-6 SEA

Anderson, E.T. and Simester, D.I., 2014. Reviews without a purchase: Low ratings, loyal customers, and deception. Journal of Marketing Research,51(3), pp.249-269.

Competition and Markets Authority, 'Online Reviews and Endorsements Report on the CMA's Call for Information' (19 June 2015)

Fei, G., Mukherjee, A., Liu, B., Hsu, M., Castellanos, M., & Ghosh, R. (2013). Exploiting Burstiness in Reviews for Review Spammer Detection. In Seventh International AAAI Conference on Weblogs and Social Media.

Fornaciari, T., dell'Interno, M. and Poesio, M., 2012. Identifying fake Amazon reviews as learning from crowds.
Li, J., Ott, M., Cardie, C. and Hovy, E., 2014. Towards a general rule for identifying deceptive opinion spam. ACL.
Ott, Myle, et al. "Finding deceptive opinion spam by any stretch of the imagination." Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1. Association for Computational Linguistics, 2011.
Yoo, K.H. and Gretzel, U., 2009. Comparison of deceptive and truthful travel reviews. Information and communication technologies in tourism 2009, pp.37-47.
Zhou, L., Burgoon, J.K., Twitchell, D.P., Qin, T. and Nunamaker Jr, J.F., 2004. A comparison of classification methods for predicting deception in computer-mediated communication. Journal of Management Information Systems, 20(4), pp.139-166.

---

**Dr Rui Sousa Silva (Universidade do Porto, Portugal**

*'A Wink's Not as Good as a Nod': a new paradigm for forensic authorship analysis?*

Cybercrime has traditionally been associated with financial crimes, such as theft of bank account and credit card details, as these are often described as the most common cyber crimes (Cibercrime, 2013). However, other types of cyber crimes using communication technologies as computers, smartphones and other wireless devices have gained visibility in recent years, e.g. for creating fake profiles in the social media (such as Facebook) for purposes of committing hate crimes, threats, slander, libel and defamation, as well as fraud, identity theft, electronic vandalism and violation of intellectual property rights – as part of both organised and unorganised crime. In most cases, the investigative process is made significantly harder by information technology strategies used by cybercriminals to ensure their anonymity, as is the case of using public access computers (such as those in cybercafés or public libraries) or IP address hide software. However, the underlying use of language in such cases makes the case for forensic linguistic analysis. In most of these cases, forensic linguists can use forensic authorship analysis and work with computer scientists in combatting such crimes: by building on the principle that every speaker or writer of a language has an idiosyncratic way of speaking or writing (Coulthard, 2004) – their own idiolect – suspects can be proved or disproved as the true authors of cybercriminal texts. Notwithstanding, given that the development of new information and communication technologies contributes to the emergence of new genres, means and modes of communication, new challenges are raised to forensic authorship analysis. This study presents some preliminary results of the analysis of real forensic texts, provided by the Portuguese Cybercrime Office. In addition to identifying and discussing the more salient markers of authorship, this paper proposes and discusses the potential and the limitations of novel approaches to authorship analysis.

*References*

Cibercrime, G. (2013). *Relatório da Actividade 2013*. Lisboa: Procuradoria-Geral da República.
Coulthard, M. (2004). 'Author identification, idiolect and linguistic uniqueness'. *Applied Linguistics*, 25(4), 431–447.