Psychiatry, Psychology and Law, 2013
Vol. 20, No. 2, 294–300, http://dx.doi.org/10.1080/13218719.2012.672274

Routledge
Taylor & Francis Group

No-one Knows You're a Dog on the Internet: Implications for Proactive Police Investigation of Sexual Offenders

Robyn Lincoln and Ian R. Coyle

Bond University, Robina Queensland, Australia

There is a body of literature dealing with the increased capacity for deception in online environments. This corpus of academic work has relevance for the widespread public concern about the anonymity of the Internet with respect to children who may be contacted by sex offenders. The present paper reports findings from a deception condition study where pairs of subjects engaged in computer-mediated interaction and were asked to evaluate the age and sex of their interlocutors. They were generally successful at this and tended to base their decisions on the content of the conversation. It demonstrates that individuals, despite the anonymity theoretically offered by the Internet, can discern the age and sex of those they are conversing with online, which has implications for police training and practice when engaged in online covert operations.

Key words: covert online investigations; Internet communication; online sex offending; police sting operations.

The use of police sting operations on the Internet to catch sexual predators is based on the presumption that covert operatives can successfully manipulate gender and age. This is arguable. This study demonstrates that individuals, despite the anonymity theoretically offered by the Internet, can discern the age and sex of their interlocutor. In doing so, they use content-based information rather than stylistic cues; this is in apparent contradistinction to the literature on Internet communication. This has profound implications for covert police operatives and suggests that training should emphasize the importance of content in Internet-based sting operations.

Investigators masquerading as children on the Internet to catch potential sex offenders is an increasingly common tactic employed by law enforcement agencies worldwide. Although the defence of role playing or engaging in fantasy has been raised in many cases overseas it has been unsuccessful (Mitchell, Wolak, & Finkelhor, 2005). In Australia, the authors are aware of only one case, *R v Plumridge* [2007] QDC, in which the defence of role playing has been successfully employed. This case raises a number of issues that are highly pertinent to the successful conduct of proactive covert operations on the Internet aimed at catching potential sex offenders.

The Facts of the Case

In July 2006, Darryl Plumridge was indicted under s 218A(1) of the *Criminal Code of Queensland*. The charge alleged

Correspondence: rlincoln@bond.edu.au

against him was based on the proposition that he believed the person with whom he was engaged in conversation on the Internet was under the age of 16 years. In fact, his interlocutor was a middle-aged male police officer. No attempt was made to contact "Erin Princess Baby" (EPB) who was portrayed as a 13-year-old female. His defence was alarmingly simple; he claimed that he knew the person with whom he was communicating was an older male and he was simply role playing. He claimed that there were a number of obvious content cues inadvertently provided by the covert police operative which would have led him to the view that his interlocutor was lying. These include the following: the capacity of EPB to "work out" how to send a file in 1 minute 11 seconds after initially saying "I have one (referring to a picture) but I am not sure how to send it"; EPB stating "she" "only knew (sic) to chat really" yet displaying significant familiarity with protocol/procedure as evidenced by "her" retort "wats (sic) with the CAPS" to the use of capitals (which are considered a form of shouting/aggression in online communication); and EPB's observation that "she" was in her office when "she" was supposed to be home from school then correcting this glaring error. He also claimed that certain linguistic cues such as the use of the terms "spaz" and "veg" and the sign off by the interlocutor "see ya later alligator" were not terms that 13-year-old females would use. These, so Plumridge claimed, further alerted him to the masquerade.

The defence hinged upon the application of s 218A(8) of the *Criminal Code of Queensland* 1896 which states (emphasis added):

> Evidence that the person was represented as being under the age of 16 years or 12 years, as the case may be, is, *in the absence of evidence to the contrary*, proof that the adult believed the person was under that age.

The application of this section had been considered in *R v Shetty* [2005] QCA 225 where it was held, per Keane JA [at 26], that: "If the adult does adduce evidence as to what he or she actually believed then it is a matter for the jury whether or not this evidence is accepted." Objections were raised by the Crown, under s 590AA of the Code, as to the admissibility of expert reports dealing with psychological and linguistic issues germane to the defendant's belief as to the age of EPB. This application was heard before Judge McGill (unreported: Queensland District Court, Brisbane, 2 May 2007). In rejecting the Crown's submissions that the proposed evidence of Professor Coyle and Dr Pensalfini was inadmissible, His Honour commented [at 1] as follows:

> Some years ago now I saw, I think in the *New Yorker* magazine, a cartoon which showed two dogs in a room, one of them standing in front of a computer terminal, and apparently saying to the other one, "On the Internet nobody knows you're a dog." There may well be a good deal of truth beneath that hyperbole, but the evidence I have to consider in this application suggests that communication using the Internet is not necessarily as anonymous as is generally believed.

His Honour went on to conclude that a psychologist would possess [at 16]:

> expertise relevant to the assessment of ability on the part of a particular person to be able to determine whether a person with whom he is in communication over the Internet is being honest in that communication, particularly in relation to the identification of gender.

He opined that a linguist's skills were relevant to assisting the jury to consider the defences propositions [at 23]:

> English usage changes over time ... Slang therefore tends to come and go ... Certainly the identification of slang which is characteristic of particular generations, or not characteristic of

> particular generations, would be something which would be too sophisticated for the average juror, and would justify expert evidence.

With that issue decided, the trial proceeded. Mr Plumridge was found not guilty.

The Relevance of this Case to Internet Stings

There is a robust and extensive literature on the factors specific to communication via the Internet (Whitty & Joinson, 2009). Factors specific to Internet communication include a lack of the non-verbal cues present in face-to-face communication; the increased latency of response; the lack of situational cues such as might be obtained from the environment where a conversation is taking place; the lack of physical cues as to the interlocutor's anthropometry, appearance, gender, age and clothing. Although emoticons (emotive icons which use a corrupted/acronymic form of language to convey meaning) are used in other forms of communication such as SMS communication, they are particularly important in communication on Internet chat rooms as they rapidly demonstrate, to one degree or another, familiarity with the jargon specific to chat rooms and familiarity with the technology involved. For example, using the emoticon "lol" (laugh out loud) demonstrates that the interlocutor is not a tyro. Similarly, being able to send the interlocutor a file containing, say, a picture demonstrates familiarity with the software involved.

Even over the telephone many cues are available that are not present in Internet chat room communication. These include changes in hesitation, pitch and intonation, which are reliable indicators of dissembling or lying (DePaulo et al., 2003; Granhag & Strömwall, 2004). Hartwig and Bond Jr (2011) have approached the problem of the detection of lying from a different perspective. They suggest that people fail to detect lies not because they do not utilize cues that are diagnostic of deception, but because the behavioural differences between liars and truth-tellers are minute. Such differences are likely to be much harder to detect over the Internet than in other forms of communication. Further, it must be considered that Internet chat room communication is essentially anonymous unless the interlocutor has extremely advanced technical skills/resources or they volunteer to give up this anonymity.

Considering these issues, it was initially posited that communication over the Internet could open up a brave new world where issues of gender, social class and race would be rendered otiose by the technology. This has proved not to be the case. As has been observed: "signalling gender is often an activity of interest online, for a variety of reasons, and ascertaining the gender of others is particularly important to users who for one reason or another doubt the sincerity of their online conversation partners" (Herring & Martinson, 2004, pp. 424–425). How can the gender of interlocutors be determined when the language used, which is usually abbreviated or largely in the form of emoticons, provides the only cues? Males make greater use of assertions, profanity, challenges, insults, self-promotion and interruptions, whereas females tend to be collaborative and to use indirect language, make more use of hedges, justifications and expressions of emotion, personal pronouns and polite language (Li, 2005; Yates, 2001). It has been argued that these cues enable discrimination of the interlocutor via gender-linked language clues (Lee, 2007).

While it is doubtless true that online gender deception is possible, it is also true that unconscious use of language and discourse styles can reveal gender when the interlocutor is trying to avoid giving off any cues (Savicki, Lingenfleter, & Kelley, 1996; Thompson & Murachver, 2001). One comprehensive study found that with males who successfully impersonated females the ratio of female to male stylistic features was 4 to 1, whereas with males who unsuccessfully tried to impersonate females the ratio was 2 to 1 (Herring & Martinson, 2004). This study is highly significant in that it was based on 2,212 "games" involving 11,158 people. Forty per cent of these games were about gender identity where individuals would deliberately try to adopt opposite gender identities. However, it is obvious that in online communication individuals also consider content when making judgements about the gender of interlocutors, especially in situations where potential subterfuge is involved as there are a number of processes which enable participants in computer-mediated interaction to manage impressions (Walther, 2007).

Despite considerable interest in the area of computer-mediated interaction, to the authors' knowledge, no study has addressed the relative importance of the content and stylistic cues individuals use in determining gender and age on the Internet in the context of police sting operations where covert operatives are attempting to portray themselves as younger persons, typically teenagers, often of the opposite sex. In fact, to the authors' knowledge, there are no studies that deal with the determination of age and gender in the context of dissembling or outright fabrication as would be expected in police sting operations. In the light of the decision in *R v Plumridge* and ongoing police sting operations this is an area of considerable importance. This study aimed to address these issues.

Methodology

Participants

The participants comprised 46 undergraduate and postgraduate students from a range of faculties at Bond University; they responded to requests for participants advertised throughout the university. Three pairs of subjects were excluded because of a failure to follow instructions or because the university intranet over which conversations were conducted failed to fully record the online chat.

Procedure

Participants, who were offered an incentive of $A20, were requested to sign consent forms to demonstrate their willingness to participate in the study. The consent form outlined confidentiality and anonymity issues: the methodology of the study was approved by the relevant research ethics committee. Separate researchers met participants at different locations on campus and escorted them to offices at different locations where they could access the university's intranet. This process permitted students to be paired in a way that precluded identification of each participant. Allocation to experimental groups was on a "first come, first served" basis; that is, students who first arrived were allocated to one group (A), and the later arrivals allocated to another group (B).

The researchers engaged in deception when briefing the participants of this study. Those in Group A ("deceivers") were instructed to play the role of a 13-year-old female whilst participating in the online chat: that is, they deliberately tried to deceive their interlocutor in Group B ("receivers") as to their age and sex. Both groups were deceived about the actual ages of the people that they were chatting with, and told that these ages ranged from young children to the elderly but no children or elderly participated in this study. Considering that "deceivers" and "receivers" could be male or female, there were four possible combinations of "deceivers" and "receivers".

After being escorted to an office containing an online computer, participants engaged in generalized text-based chatting with another participant for a maximum of 30 minutes. Participants were instructed that the topic of discussion was open to participants; for example, plans for the weekend, life in general and hobbies. It was a requirement that participants not engage in communication that could be considered defamatory, racist and sexist or in any other way discriminatory. The Bond University intranet includes a chat room discussion facility with the capacity to record "chat" and all conversations were recorded for subsequent analysis. After completion of online interaction, participants were given a questionnaire to complete. Neglecting demographic variables, which are self-explanatory, the salient items of the questionnaire in the context of this study were concerned with the participants' Internet experience and their reasons for assigning age/sex to their interlocutors. Participants were then debriefed and the deception that was employed in the study was explained. No participant reported any negative consequences arising from the study. Finally, the participants were reassured that the data were confidential.

Results

Participant ages ranged from 18 to 38 years ($M = 23.25$; $SD = 5.52$). Male participants' ($n = 20$) ages ranged from 18 to 36 years ($M = 22.35$; $SD = 4.89$). Female participants' ($n = 20$) ages ranged from 18 to 38 years ($M = 24.15$; $SD = 6.08$).

Preliminary data analysis revealed that no reliable categorization of participant's rationale for assigning sex/age to their interlocutor could be made apart from the broad categories of style of communication (e.g., use of emoticons, syntax, colloquialisms, neologisms) or the content of the communication (e.g., chatting about football teams, shopping or television shows). Similarly, preliminary analysis indicated that there was no difference between the four data cells of "deceivers" and "receivers" (M/F; M/M; F/F; F/M). Accordingly, the cells were collapsed for final analysis. Because the data were in the form of a dichotomous, nominal, distribution (correct–incorrect) the cumulative binomial distribution test (Stattrek.com) was utilized for data analysis. The age of their interlocutors estimated by "receivers" ranged from 18 to 39. Because a number of participants provided an age range rather a discrete age (as the instructions indicated) it was not considered meaningful to derive measures of central tendency. Based on preliminary analysis, in determining whether or not "receivers" were able to identify their interlocutor's age correctly, five-year bandwidths ranging from 11 years onwards were employed as well as whether the "receivers" indicated that their interlocutor was under the age for consensual sex of 16 years mandated by legislation throughout Australia.

Inter-judge concordance, based on independent coding of the data by the authors and a research assistant for assessment of content or style-based cues for gender and age of the "deceivers" by the "receivers" was 85% and 100%, respectively. In cases where all three judges did not agree the majority rating was used for further analysis.

The proportion of correct identifications of gender and age (based on five-year bandwidths) of their interlocutors by the "receivers" was, respectively: 16/20 ($p = 0.999$) and 15/20 ($p = 0.994$). The proportion of the "receivers" who correctly identified both the gender and age (based on five-year bandwidths) of their interlocutors was 12/20 ($p = 0.868$). None of the "receivers" identified their interlocutor as being under 16 years of age. The proportion of "receivers" employing content and style-based cues to determine the gender of their interlocutors was, respectively, 16/20 ($p = 0.999$) and 4/20 ($p = 0.006$). The proportion of “receivers” employing content and style-based cues to determine the age of their interlocutors was, respectively, 13/20 ($p = 0.942$) and 7/20 ($p = 0.132$).

Discussion and Conclusions

The finding that individuals in computer-mediated interaction overwhelmingly decided the gender and age of their interlocutor on the basis of the content of the discussions, on the surface, contradicts the findings of previous studies. But this contradiction is more illusory than real since no-one has asked the questions addressed by this study. Accordingly, the results of this study do not show that stylistic cues are not important. They are, but cues derived from the content of the communications are perceived as being more important, at least within the context of this study.

The finding that none of the “deceivers” were able to convince their interlocutors that they were a 13-year-old female is noteworthy and raises the question as to whether the participants in this study are representative of the population of potential Internet sexual predators. Given the enormous diversity of such predators that have been caught in Internet sting operations (Mitchell et al., 2005), it is unreasonable to argue that tertiary study, albeit uncompleted for the majority of participants in this study, is proof against sexual offending on the Internet. Nonetheless, like Mr Plumridge, the participant’s IQ is certainly well above the norm and this may have been a factor in enabling the “receivers” to discriminate that their interlocutor was not 13 years of age, or even under 16 years of age. A more prosaic explanation is that content cues provided by the “deceivers” may have given the game away, as they clearly did with respect to the assessment of gender.

It is well established that more accurate decisions and judgements about deception can be made if and when people consider more than one piece of evidence. However, cognitive biases such as confirmation bias and anchoring bias act to prevent people considering all available evidence when making truth/lie judgements (Porter & ten Brinke, 2010; Vrij, 2004). These biases influence people to only consider evidence that confirms their initial assessments or hypotheses. This has important ramifications for covert operations designed to catch potential sex offenders (Krone, 2005). Utilizing cognitive biases by ensuring that content and response style are consistent, ab initio, with what the interlocutor would expect of a child of the presumed age and sex is likely to be an effective means of forcing the initial decision (i.e., whether the interlocutor is a covert operative or not).

This suggested approach involves turning the vast body of research into detection of deception in forensic contexts on its head. Rather than asking how people can detect deception in the context of Internet sting operations we should be asking: how can covert operatives become better liars? First, it is clear that covert operatives must be familiar with content information that the gender and age group they are attempting to portray would be expected to know. This could be obtained in any number of ways such as reading magazines and watching television programmes appropriate to the age and gender of those whom they are attempting to emulate. Alternatively, operatives charged with this difficult task could be sent to observe and interact with adolescents at school and other social venues, required to undertake texting sessions with children of the same demographic they are attempting to emulate or spend time speaking/interacting with children representative of this demographic. This is unlikely to prove popular with covert police operatives, but it would, we suggest, be highly effective.

Equally, it is clear that familiarity with chat room protocol and the application of the software utilized in chat room communication is fundamental to the capacity to detect lying/dissembling of any kind. For example, if an interlocutor claims to be a tyro with computers and the means of sending a file (which may take hours to learn) yet is able without specific instruction to respond within a minute or two this would indicate that they are lying about their level of knowledge of the procedure/protocol involved.

Finally, this study shows that individuals can discern the age and gender of their interlocutor within a relatively brief period. Thus for some individuals, the defence employed by the accused in the matter of *R v Plumridge* has scientific justification, with caveats. In particular, glaring content errors, such as claiming to be off school but then stating the "she" was in the office, as happened in the Plumridge case, will give the game away much more readily than syntactical and other stylistic errors.

References

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin*, *129*(1), 74–118.

Granhag, P. A., & Strömwall, L. A. (Eds.). (2004). *The detection of deception in forensic contexts*. Cambridge: Cambridge University Press.

Hartwig, M., & Bond Jr, C. F. (2011). Why do lie-catchers fail? A lens model meta-analysis of human lie judgements. *Psychological Bulletin*, *137*(4), 643–659.

Herring, S. C., & Martinson, A. M. (2004). Assessing gender authenticity in computer-mediated language use. *Journal of Language and Social Psychology*, *23*(4), 424–446.

Krone, A. (2005, July). Queensland police stings in online chat rooms. *Trends and Issues in Crime and Criminal Justice*, *301*. Canberra: Australian Institute of Criminology.

Lee, E-J. (2007). Effects of gendered language on gender stereotyping in computer-mediated communication: The moderating role of depersonalization and gender-role orientation. *Human Communication Research*, *33*, 515–535.

Li, Q. (2005). Gender and CMC: a review of conflict and harassment. *Australasian Journal of Educational Technology*, *21*(3), 382–406.

Mitchell, K., Wolak, J., & Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working? *Sexual Abuse: A Journal of Research and Treatment*, *17*(3), 241–267.

Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high stakes deception? *Legal and Criminological Psychology*, *15*, 57–75.

Savicki, B. W., Lingenfleter, D., & Kelley, W. G. (1996). Gender language style and group composition in Internet discussion lists. *Journal of Computer Mediated Communication 2*(3).

Stattrek.com. http://stattrek.com/online-calculator/binomial.aspx

Thompson, R., & Murachver, T. (2001). Predicting gender from electronic discourse. *British Journal of Social Psychology*, *40*, 193–208.

Vrij, A. (2004). Why professionals fail to catch liars and how they can improve. *Legal and Criminalogical Psychology*, *9*, 159–181.

Walther, J. B. (2007). Selective self-preservation in computer-mediated communication: Hyperpersonal dimensions of technology, language and cognition. *Computers in Human Behaviour*, *23*, 2538–2557.

Whitty, M. T., & Joinson, A. N. (2009). *Truth lies and trust on the Internet*. New York: Routledge.

Yates, S. (2001). Gender, language and CMC for education. *Learning and Instruction*, *11*, 21–34.