COVER PAGE

Submission to: *Psychology Teaching Review* Special Issue on 'Teaching sensitive issues in psychology'

Title: Teaching Sensitive Issues in Cyberpsychology

Authors: Jacqui Taylor*, John McAlaney, Sarah Muir & Terri Cole

*corresponding author jtaylor@bournemouth.ac.uk

Affliation: Dept Psychology, Faculty of Science & Technology, Bournemouth University, Poole, UK

Category of submission: Debating points [2000 to 4000 words]

ANONYMISED SUBMISSION

Teaching Sensitive Issues in Cyberpsychology

Abstract

In contrast to the helpful sources of guidance and regulations for researchers designing and conducting experiments in cyberpsychology, there is very little guidance available for academics and teachers teaching sensitive issues related to behavior in the online world. There are many potential dangers for psychology students when learning about cyberpsychology, ranging from being exposed to upsetting or illegal behavior viewed in videos or images, to questioning their own sense of morality and understanding of self, to experiencing harassment or hacking. This paper will highlight our own experiences of teaching cyberpsychology to first and third year psychology students, highlighting some of the potential dangers. We suggest recommendations for academics to ensure that students are protected as far as is possible.

1.0 Introduction

There is no shortage of research investigating the impacts of technology and the internet and many sensitive topics are explored in this research (e.g. Attrill, 2015). Online research can pose many challenges in adhering to existing ethical principles in Psychology (BPS, 2014) and in 2013, the BPS published 'Ethics Guidelines for Internet-mediated Research' to address these challenges. However, although some of these principles are relevant to both teaching and research, there is very little ethical guidance specifically for teachers of cyberpsychology.

There are many potential dangers for psychology students when learning about cyberpsychology. The many examples of students and children being exposed to upsetting or illegal videos and images during online researching are identified by the extensive European-wide review and survey conducted by Livingstone, Haddon, Görzig and Ólafsson (2011). However, less visible and under-researched impacts also include students questioning their own moral compass and understanding of their self or identity when engaging with sensitive materials online. Negative communication such as harassment or hacking may be experienced following participation in social media (such as posts or tweets). Examples of these emotional, behavioural and cognitive effects will now be discussed.

This article will highlight our experiences teaching cyberpsychology to undergraduate psychology students and will discuss the ways that we have guided and supported them. Section 2 is divided into three parts: section 2.1 will explore the motivations that lead to people behaving in a deviant or deceptive way online; next (section 2.2) we explore the impacts of the internet on individuals and cover the topics of cyberbullying, cyber-harassment, trolling, online health and sexual behavior; finally in section 2.3 we discuss many of the moral and legal issues involved when teaching cybersecurity. In section 3, we summarise our recommendations for academics to help to ensure that students are supported and protected when learning about sensitive issues in the online world.

2.0 Examples of teaching sensitive issues relating to the psychological and social impacts of the Internet

We will highlight our experiences teaching sensitive issues to undergraduate psychology students; the majority of examples come from experiences within our final year unit 'Cyberpsychology', but also from teaching a guest lecture on a 1st year unit on 'Current Issues in Psychology' and other final year units in 'Forensic Psychology' and 'Health Psychology'. Within each section we suggest ways that we have protected, guided and supported students with the specific issues that could arise.

2.1 Exploring why people are deviant or deceptive online

One of the areas that researchers have investigated is the motivations behind online deviance. A number of approaches exist, each focussing on different aspects to explain deviant behaviour; some approaches draw on the media, others on the group context and others on individual characteristics. Suler (2004b) identifies the 'online disinhibition effect' to explain many of the effects and this approach has been applied widely over the last 15 years.

Teaching and learning mainly took place through online asynchronous discussions within a 3rd year Cyberpsychology unit. Before teaching began the following text was placed on the presentation slides 48 hours prior to the lecture warning of the material to be covered:
'When researching the topic of deviance, please be mindful that online searching could result in things you wish you had not seen. Therefore, please think carefully regarding your search terms, consider filters and think carefully before clicking on any links. Remember your digital path can always be tracked. If you do come across anything which makes you feel uncomfortable, please inform the appropriate service (such as CEOP, IT support) or discuss with BU counselling.'
Issues that were debated within the online discussions included: differences between online and offline deviance; online identity deception and persuasion involved in grooming or scamming, and Munchausen by Internet (MBI) where fake sufferers discuss their illnesses via social media (Pulman & Taylor, 2012).

Online student discussions have many advantages over face-to-face discussions in teaching (Taylor 2002), especially if students can communicate separated by space or time (i.e. asynchronously). For example, they encourage more interactivity and are less likely to be dominated by one or two students, compared to face-to-face discussions (Herring & Stoerger, 2014). Although not anonymous, online discussions provide a forum where it is possible for students to be less inhibited. Suler (2004a) defines this as the 'online disinhibition effect' because without having to deal with face-to-face encounters, people can express themselves more openly. Students who are socially anxious often find online discussions to be more enjoyable (Taylor, 2002) as they reduce anxieties around negative evaluation from others. Asynchronous online discussions can allow students to be their true selves, however this does not come without risks relating to self-disclosure and therefore students need to be warned about this possible effect and the online discussion board should be set up so that students can delete their own messages. Savin-Baden, Tombs, Burden and Wood (2013) investigated student disclosure when they were asked to respond candidly to a lifestyle choices online survey and found correlations between a user's sense of trust, levels of truthfulness and engagement. An issue for future consideration is that as students took part in the online discussions asynchronously they may not have support available should they experience an

uncomfortable topic or feeling. Many students participated outside of the working day, often late at night, when tired or potentially under the influence of alcohol or drugs which could affect perceptions or behaviour.

The wider issue of morality in videogames provoked much discussion. Videogames now have advanced graphics so that for many players the gap between reality and fantasy is closing; the impact of playing *through* a character in first person shooter type games means that players can control or act out behaviours. These behaviours can be illegal, although Gibbons (2009) proposed that avatar activity was only illegal if it affected real life. Despite this, cognitive, emotional and behavioural components of morality are observed in videogames: players make moral choices, act out behaviours, and are emotionally involved with a character. As we will see later in section 2.3, although there are many laws which students need to know about regarding what is wrong or right online, there are not many things that are ethically questionable that are not illegal (and possibly vice versa!).

2.2 Exploring the impacts of the internet on individuals

In this section we discuss the impacts of the internet on individuals and highlight where we help to warn and protect students who may have experienced some of these effects. We cover the topics of cyberbullying, cyber-harassment, trolling, online health and sexual behavior.

2.2.1 Cyberbullying, cyber-harassment and trolling

Cyberbullying involves the use of mobile phones, computers, social networks and other forms of digital technology to repeatedly and intentionally intimidate, humiliate, tease or upset a young person. The cyberbully is usually invisible or anonymous and the impacts can be different from traditional bullying as it reaches a far greater audience, involves more people and can occur 24 hours per day and is therefore hard to get away from. Cyber-victims are less likely to report bullying or seek help than traditional victims. Cyber-harassment (often in the form of trolling) involves adults, rather than children, and is motivated by a desire to control, intimidate or influence another. According to Buckels, Trapnell & Paulhus (2014), trolling is "the practice of behaving in a deceptive, destructive, or disruptive manner in a social setting on the Internet, for no purpose other than their pleasure". Buckels et al relate three psychological traits to those who partake in trolling (sadism, psychopathy, narcissm) and it is possible that when students research these traits (especially sadism) they will come across unpleasant images. It is useful to provide students with examples to illustrate safe examples plus more extreme examples of each of these traits.

Teaching and learning of this topic took place through a guest lecture on a first year unit 'Current Issues in Psychology'. Before teaching began, the following text was inserted on the first slide of the presentation uploaded 48 hours prior to the lecture warning of the material to be covered:
'Cyberbullying/harassment may be a sensitive issue for some of you (around 1 in 4 people have personally experienced it). Many sources of support are discussed within the lecture and should you need to discuss your feelings or concerns with somebody please contact these sources.' The lecture covered real cases (the case of a teenager Izzy Dicks who committed suicide after cyberbullying) and the effects on both the victim and their family and friends. Naturally this covers issues such as suicide and self-harm which needs to be handled sensitively. At the end of the lecture, students were once again provided with sources of support.

2.2.2 Online health

Although online health websites are widely available, there are many issues of concern such as: inaccurate or irrelevant information; lack of interactivity; and potential harm due to the ease of students to stumble across sites with negative intentions (Kanuga & Rosenfeld, 2004). Teaching and learning of this topic took place through lectures and seminars on the third year 'Health Psychology' and 'Cyberpsychology' units. A number of health topics are covered (e.g. online addiction, gender identity, sexually transmitted disease), but space precludes a full discussion of all these and instead we focus on the issue of eating disorders.

Pro-anorexia is a good example for demonstrating the principles of online communities as they involve a number of people engaging in ongoing interaction and relationships with others who share a passionate belief about a topic (Kim, 2000). They also provide a good topic for students to engage in healthy debate. Csipke and Horne (2007) report that media representations of pro-anorexia are sensationalizing and are often a key motivator for people to visit the sites. Thus, the first part of the lecture includes a critical evaluation of the discourses conveyed in the media and highlight the inaccuracies conveyed (i.e. that the websites do not give people eating disorders or try to 'recruit' anorexics!). We then focus on a reason that people use pro-anorexia websites, i.e. as a way of communicating with others who also see their eating disorder as a coping mechanism or playing some other functional role (Williams & Reid, 2007) and as a 'safe' sanctuary for those working through ambivalent feelings about their eating disorder whilst being encouraged to recover if this is what they want to do (Brotsky & Giles, 2007). Throughout the lecture no names of communities are given, images are censored or left out and links for resources for support are given at the end. However, we believe that by focusing on the research evidence relating to pro-anorexia, rather than the media's representation (and quelling some of the myths in the process) the topic is covered in a much safer way. More generally, when covering the topic of eating disorders we are mindful that students may be experiencing an eating disorder themselves or know or suspect peers or friends who are suffering; again we provide many sources of support involving face-to-face, telephone and websites.

2.2.3 Sexual behavior

Teaching and learning of this topic took place during the third year 'Forensic Psychology' and 'Cyberpsychology' units. A number of sensitive issues are covered including the relationship between sex offending and online porn, sexting, revenge porn and online misogynistic communications. To support one lecture, a film showing psychological techniques for grooming was followed by students discussing the dangers that young people may be exposed to when using the Internet. Students were asked to consider UK and international legislation and then explored educational moves to protect children. This led to wider discussions about the growing trade in indecent child images from adults and also the exchange between children in the form of sexting.

An area of teaching which required specific consideration regarding this topic was in relation to supervision of final year projects. Obviously the majority of students wish to complete projects that are of particular interest to them and these can involve sensitive topics; sometimes this interest stems from personal involvement or victimisation, for example in relation to sexting behaviour or revenge pornography. Whilst not wanting to dampen enthusiasm for research topics of interest, staff were reminded of their duty of care for

students. As such open and honest communication is essential, within an environment of professional collaboration and sharing where *all* factors which may impact the study (and any disagreements or misunderstandings) are openly discussed. In particular students were explicitly asked if there was anything the supervisor should be made aware of in their personal background which may affect their considerations. It can be explained to the student that whilst we do not want to restrict research interests, their aim is to learn to become objective scientists and as such any potential bias/preconceptions should be explicitly articulated. In addition giving students different options is suggested – they can talk to the supervisor or others, consider an alternate project, amend the current one, code data in the presence of the supervisor, have more frequent supervision. Joint decision making should be encouraged where possible. Personal reflections can be used by means of example to demonstrate the vulnerability of all involved in such research, e.g. "*with me one day it was something innocuous – a victim had the same birthday as a good friend –it really upset me and got me thinking".* These can be used to highlight that such feelings and empathy are normal, but the student needs to be reminded that they must discuss situations if they occur. Such projects also require an enhanced level of guidance in relation to specific ethical considerations – for example ensuring all participants are adult by utilising university populations and considering conducting pen and paper surveys, rather than online questionnaires via social media.

2.3 Cybersecurity

Many cybersecurity incidents are based around psychological manipulations of either the gatekeepers of secure systems or the victims directly; one of the most common examples being phishing emails. Within the field of computing these techniques are referred to as social engineering which involves the application of psychological theory, particularly those from social, consumer and cognitive psychology. Teaching psychology students about how their skills can be applied to cybersecurity has some risks. It may involve introducing them to topics and activities of varying legality that they themselves may decide they wish to be involved in. This could include clear cybercriminal activities such as obtaining credit card details, or it may involve behaviours such as hacktivism, which refers to using online technologies as a form of social protest to, for example, disrupt a website. This latter type of activity may be something that social science students such as psychology students may be especially likely to decide they wish to engage with. By its nature hacktivism often involves a minority group presenting itself as being in competition with a larger oppressor, whom the hacktivists typically portray as being unethical in nature. Examples would include multinational companies or foreign governments who may been seen to act in an unethical way. It may be difficult for students to remain impartial in these situations. Even if a student only intends to explore this phenomenon for research purposes they may inadvertently place themselves at risk. The actions associated with hacktivism are often illegal and, whilst the damage contributed by each individual involved may be relatively low, it has been suggested that some targeted organisations have aggressively pursued legal action against any individuals (many of whom are college students) who are involved in any way in these activities (Olson, 2012).

Teaching this topic also involves exposing students to technologies and activities that they may not be aware of. This includes the dark web, which refers to a part of the Internet than cannot be accessed through well-known browsers such as Chrome or Internet Explorer. Instead it can only be accessed using specific software such as Tor. When correctly used, this software can be used to preserve anonymity in a way that is not possible when using other

web browsers. Use of this software is not in itself illegal – indeed it was developed by United States Naval Research Laboratory and is used by government agents, journalists and others as a way of communicating securely and secretly (Bartlett, 2014). However, the dark web includes a number of sites which include highly illegal and potentially distressing material, including sales of illicit drugs and child pornography. The dark web is not as user friendly as the surface web and as a result there can be little indication of what a website contains before a link on the dark web is opened. An inexperienced user could for instance easily and unwittingly open a child pornography website.

Teaching and learning of this topic took place through lectures and seminars on the third year 'Cyberpsychology' unit. To prepare students for this topic the teaching sessions begins with a clear and direct explanation of the risks involved in engaging with the behaviours that were to be discussed and presented. Students were reminded that crimes committed online such as fraud are treated as seriously as offline crimes. Similarly, examples are given of individuals, specifically students, who took part in hacktivism campaigns for ideological reasons (with no financial gain) who were subsequently arrested and prosecuted. Nevertheless no statement is made to the students about what they should or should not be involved in online. If a student were to be interested in hacking and hacktivism, or indeed is already involved in these activities, then a perception that the lecturer is attempting to impose their own value system may alienate the student, particularly given that it has been argued that people involved in hacktivism are characterized by an anarchistic style (Olson, 2012). Instead, it is emphasised to the students that the onus is them to understand what the risks are and what the consequences of their actions may be. The dark web is also discussed with students, again in a very direct way in which the potential risks are highlighted. Screenshots of dark web indexes are shown in the lecture to give students an understanding of how the technology works, and also what types of site may be available on the dark web. The dark web is not itself opened in the lecture, since the nature of it is such that it can be difficult to predict what content will be visible at any one point.

3.0 Suggestions for consideration by the psychology teaching community

An environment needs to be created that allows students to safely reflect on and explore their understanding of sensitive issues. In considering the importance of individual's own behaviour and their understanding of the implications and consequences of their behaviour, students may experience self-doubts or negative self-esteem. In a safe environment, students should feel comfortable to say if something is upsetting. It is important to acknowledge that students may have been personally victimised which may affect them personally, and academically (i.e. not being able to be an objective scientist). It may be helpful for the educator to incorporate their own personal experience to encourage discussion (e.g. I was once upset reading), while being aware of students self-disclosing accidentally and being able to deal with this if it does occur.

It is important to consider stage of moral development and life experience of students when presenting sensitive materials. Educators often try to advance students' sense of moral development and reasoning (Kohlberg & Kramer, 1969), and with this in mind it is important to consider the age and experience of students when covering sensitive issues. Gibbs et al (1992) suggest undergraduates' moral development is not fully developed; they are still developing an understanding of how moral issues may relate more generally to societal functioning. Third year students may be more interested in the philosophical debates

regarding the psychological implications of Internet use and may be more open to different perspectives than first year students, having stronger convictions formed or life experiences to inform understanding. While first year students may just focus on incidences of a behavior and the legality of certain acts.

It is important to provide health warnings of what will be covered or discussed so that they essentially provide informed consent to attend. Students should be given options (e.g. to leave the class or to not attend in person). Academics should explain and discuss teacher's duty of care and potential impact on students. Sources of support should be provided before and at the end of teaching and ideally the option to talk to the lecturer afterwards.

In summary, it is impossible to provide full protection for students researching topics cyberpsychology, but as educators what we can do is to prepare students and provide guidance and support. We hope that this article contributes to the discussion and suggest that further more formal recommendations from the teaching community and professional bodies may be helpful.

References

Attrill, A. (2015) *Cyberpsychology*. Oxford: Oxford University Press.

Bartlett, J. (2014). *The Dark Net*. London: William Heinemann.

BPS (2013). *Ethics Guidelines for Internet-mediated Research*. Retrieved on 18/2/17 from the BPS website: https://beta.bps.org.uk/sites/beta.bps.org.uk/files/Policy%20%20Files/Ethics%20Guidelines%20for%20Internet-Mediated%20Research%20%282013%29.pdf

BPS (2014). *Code of Human Research Ethics*. Retrieved on 18/2/17 from the BPS website: http://www.bps.org.uk/system/files/Public%20files/code_of_human_research_ethics_dec_2014_inf180_web.pdf

Brotsky, S. R. & Giles, D. (2007). Inside the "pro-ana" community: A covert online participant observation. *Eating Disorders*, 15, 93-109.

Buckels, E.D., Trapnell, P.D. & Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and Individual Differences*, 67, 97-102.

Csipke, E. & Horne, O. (2007). Pro-eating disorder websites: Users' opinions. *European Eating Disorders Review*, 15, 196-206.

Gibbons, L. J. (2009). Law and the emotive avatar. *Vanderbilt Journal of Entertainment & Technology Law*, *11*(4), 899-920.

Gibbs, J. C., Basinger, K. S., & Fuller, D. (1992). *Moral Maturity: Measuring the development of sociomoral reflection*. Hillsdale, NJ: Erlbaum.

Herring, S. C., & Stoerger, S. (2014). Gender and (a)nonymity in computer-mediated communication. In S. Ehrlich, M. Meyerhoff, & J. Holmes (Eds.), *The Handbook of Language, Gender, and Sexuality,* 2nd edition (pp. 567-586). Chichester: John Wiley & Sons.

Kanuga M & Rosenfeld W.D. (2004). Adolescent sexuality and the internet: the good, the bad, and the URL. *Journal of Pediatric & Adolescent Gynecol.,* 17(2),117-24.

Kim, A. J. (2000). *Community Building on the Web: Secret strategies for successful online communities*. Berkeley, CA: Peachpit Press.

Kohlberg, l. & Kramer, R. (1969). Continuities and discontinuities in childhood and adult moral development. *Human Development,* 12, 93-120.

Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. Retrieved on 18/2/17 from website: http://eprints.lse.ac.uk/33731/

McGinn, M. & Arnedillo-Sánchez, I. (2015). Towards supporting communication in relationship and sexuality education through a VLE. Paper presented at the *International Conference on Cognition and Exploratory Learning in the Digital Age*. Maynooth, Ireland, October 24-26.
Olson, P. (2012). *We are Anonymous*. New York: Back Bay Books.
Pulman, A. & Taylor, J. 2012. Munchausen by Internet (MBI). *Journal of Medical Internet Research. 14(4), e115* doi:10.2196/jmir.2011
Rheingold, H. (1993). *The Virtual Community*. Cambridge, MA: MIT Press.
Suler, J. (2004a). In class and online: using discussion boards in teaching. *CyberPsychology & Behavior,* 7(4), 395-401.
Suler, J. (2004b). The online disinhibition effect. *Cyberpsychology & Behavior, 7*, 321–326.
Savin-Baden, M., Tombs, G., Burden, D. and Wood, C. (2013). 'It's Almost Like Talking to a Person': student disclosure to Pedagogical Agents in Sensitive Settings. *International Journal of Mobile and Blended Learning*, 5 (2), 78-93.
Taylor, J. (2002). A review of the use of asynchronous e-seminars in undergraduate education. In Hazemi, R., Hailes, S. and Wilbur, S. (Eds.), *The Digital University*, pp. 125-138. London: Springer-Verlag.
Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology Behavior and Social Networking*, 17(3), 131-132.
Williams, S. & Reid, M. (2007). A grounded theory approach to the phenomenon of pro-anorexia. *Addiction, Research & Theory*, 15(2), 141-152.