Justice Committee

Offensive Behaviour at Football and Threatening Communications (Scotland) Bill

Written submission from Professor William J Buchanan

1. I am a Professor of Computer Security and Digital Forensics, and would like to make comment on Section 5) Threatening Communications. My main points are:

2. Credibility of any information gained from Web posts or from electronic communications. The current Internet infrastructure, and the protocols that it uses, cannot guarantee that any posting or electronic communication can be taken on face value.

3. Lack of a strong understanding of the Internet across Law enforcement in Scotland. There does not seem to be an extensive understanding of the Internet and its operation within law enforcement in Scotland, and thought needs to be given to creating a more extensive understanding of operation of the Internet, and in the usage of electronic communications. This possibly requires creating an infrastructure in Scotland which includes a wide range of knowledge, in order for law enforcement to gain best advice on the strengths and weaknesses of any information gain, especially in cross-correlation of evidence trails.

4. Lack of enforcement around Web postings and electronic communications which are hosted or sourced from outside the UK. Many sources of Web postings, such as for Twitter and Facebook, and for electronic communications, such as for Hotmail and Google Mail, are hosted outside the UK, and they often abide by the laws for the county in which the organisation is hosted. It can thus be costly to prosecute to reveal identities those who originate suspected Web postings or electronic communications. On face value, it cannot be assumed that the source of a posting is necessarily the person who seems to be identified by the user's online identity.

5. Lack of credibility in the sender and source of email messages. There is a lack of credibility in electronic mail communication, and this cannot be used as a sole source of evidence, and needs a great deal of corroboration of other sources of evidence. Some though needs to be give about the actual details of recording the details of electronic mail communication to trace the actual source of the communications, and on the risks of spoof and spam emails.

6. The “Bot-did-it” defence. There are many pieces of malicious programs on the Internet, and these can be used to do things on behalf of a user, without their control. Along with this a suspect could also give a defence that a malicious program infected their computer and did the actions.

7. Lack of scientific rigour in the collection, preservation, analysis and reporting of digital information. Digital data is fragile, and can be easily damaged and
compromised, thus the Bill may give Scotland an opportunity to share information between law enforcement, academic and industry, in creating best practices for investigating crimes related to the Bill, and scale this to other cybercrime related activities.

8. **Lack of understanding of identity.** Online identities are often managed in a different way to the way they are done within the real world. At present many computer system have low levels of identity checking, and thus even if a user has logged into a system, does not necessarily mean they actually did this.

9. **Lack of trust from the general public.** There could be a perception within the Bill that all Web postings and electronic communications could be listened-to by the Police, as many things could relate to the focus of this Bill. A strong investigation framework and auditing system is thus required so that the Bill is not abused by allowing for all Web postings and electronic communications to be investigated, even if they are intended to be private.

10. **Mistaken posting, errors, and slips-off-the-tongue.** The Internet is prone to many human weaknesses of being too fast to respond to things, or posting something which was not actually intended. Along with this human tend not to fully understand the new Internet methods, and can make mistakes, such as in forwarding postings to others by mistake, or to an incorrect email recipient.

11. **Lack of the opportunity to remove inappropriately posted/ emailed messages.** With the speed of response of user posting things to forums or Web sites, or in texting/emailing, users can often react too quickly to an event, and then have very little opportunity to recall it.

12. I would strongly recommend that a cross-domain team is setup related to the Internet and electronic communications in Scotland, which provided the framework for any related investigation, which defends the rights of society as defined in the Bill, but also protected the rights of the individual to privacy. This could include law enforcement, academia and industry within Scotland, and which could inform further bills in related areas, and allow Scotland to lead the world in these areas.

**Key Points**

13. I am a Professor of Computer Security and Digital Forensics, and lead the Scottish Centre of Excellence in Computer Security and Cyber. We work extensively with a range of collaborators on the areas of computer security, digital forensics and cybercrime, including with the Scottish Police. The main comments of this document relates to Section 5) Threatening Communications, as the focus of this includes the usage of the Internet, typically with Web-based posts and electronic communications – see Paragraph 1.

14. While the Bill is a step in the right direction that integrates traditional offensive behaviour with the equivalent with electronic communications. The major problem with
including Internet-based communications and postings, is that the Internet does not have a sound infrastructure for the overall creditability of the any original sources of information. For example there are many examples of spoof postings, where users can use aliases or identities that can be identified with others. This can be done for many reasons, including malicious intents or even with bribery – see Paragraph 2.

15. The current experience within the Scottish Police related to Cybercrime is strongest within small pockets of expertise, such as within the Scottish Crime and Drug Enforcement Agency (SCDEA), but there is a lack of general skills and understanding of the Internet within Law Enforcement in Scotland, and, to a certain extent, over the UK. A key focus for this Bill is therefore to create an infrastructure within Scotland which includes a range of domains, and which is creditable in both protecting society and also preserving the rights of the individual – see Paragraph 3.

16. Many of the Web sites related to electronic posts are not actually based in Scotland or even in the UK. Thus the laws related to releasing information about the actual identity of a person posting a message might be difficult. It might also be difficult to prostitute as the methods of registration onto a Web site might be difficult to actually verify – see Paragraph 4.

17. A particularly difficult area is in tracing the source of an e-mail, as there is often no check on the original sender of an email, where any email address can be given in the sender address. Along with this, proxy email systems can often used to hide the original sender and their location. An email is thus often difficult to trace as the protocols used are fairly archaic – see Paragraph 5.

18. There are many risks on the Internet at the present such as for “Bots” or Trojan Horse programs which can do malicious things on behalf of the user. If this is true, then there needs to be thought about how this could be proven. Along with this, the suspect could use defend themselves with a claim that they had a Trojan horse project which did the malicious behaviour – see Paragraph 6.

19. As with any form of crime related to digital communications, there is a danger that investigations might not be properly defined with a lack of strong scientific methodology, where the evidence is compromised in some way. The Bill gives us the opportunity to refresh the methodologies used for evidence gathering in Scotland, with the possibility of knowledge exchange from academia and industry, to create best practice for the collection, preservation, reporting and analysis of digital information – see Paragraph 7.

20. A major problem on the Internet at the present time is that user login names and passwords are often easily guessed, and malicious persons can often gain the details of a person, and use their account for their own purposes. As passwords become difficult to manage, many users write them down, or they can be easily guessed by people who know them, thus the credibility of users, even if they have logged in and have been authenticated, could be called into question – see Paragraph 8.
21. There is a risk in the Bill, if the investigation system is not open and well defined, that the general public will feel that the police are spying on their postings and investigating their emails, by justifying it though this Bill. A clear investigation framework and associated independent auditing is thus required in order to increase trust in the Bill – see Paragraph 9.

22. Unfortunately the Internet allows for the fast spread of communications, which could be posted or written in mistake, thus there is a risk around people reacting too quickly or incorrectly, without any real intention. Along with this, the meaning of a posting or electronic communication can often be interpreted incorrect, where a joke can be taken seriously. Without any associated body language, it can be difficult to actually interpret the intent behind an electronic message – see Paragraph 10.

23. Related to this, is that people often post things to the Internet or send inappropriate emails, which they regret later. Unfortunately it is often extremely difficult to recall email messages (as most systems do not properly support this), and messages posted on forums, are often difficult to actually remote, as there is a lack of contact details. With the speed of postings with mobile phones and the quickness of postings, a user can often react too quickly and often regret, with little chance of recalling it – see Paragraph 11.

**Author Background**

Bill Buchanan is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS (British Computer Society) and the IET (Institute for Engineering and Technology). He currently leads the Centre for Distributed Computing, Networks, and Security, and works in the areas of security, next generation user interfaces, Web-based infrastructures, e-Crime, intrusion detection systems, digital forensics, e-Health, mobile computing, agent-based systems, and simulation. Bill has one of the most extensive academic sites in the World, and is involved in many areas of novel research and teaching in computing. He has published over 27 academic books, and over 130 academic research papers, along with awards for excellence in knowledge transfer, and for teaching. His publications include the Handbook of the Internet, and the Handbook of Data Communications and Networks, along with a forthcoming book on the Handbook of Computer Security.

Presently he is working with a range of industrial/domain partners, including with the Scottish Police, health care professionals and the FSA. As part of the drive to create a World-leading infrastructure for security and cybercrime, he leads the Scottish Centre of Excellence for Security and Cybercrime which bring together a wide range of collaborators, including most of the universities in Scotland, the Scottish Police, the public sector, and a range of SMEs and large organisations. At present he is a Knowledge Transfer Lead for the Investigation and Evidence Network of the Scottish Institute for Policing Research (SIPR).
He has a long track record in commercialisation activities, including being a co-founder of Inquisitive System, which has progressed from PhD work to a university spin-out. This spin-out has also involved patenting novel security software in three countries around the World. His current work includes a collaboration with Microsoft plc on a £2million project which aims to improve the care of the elderly using Trusted Cloud-based services, and with Chelsea and Westminster Hospital on a next generation Health Care platform. This also matches up with other funded projects with the FSA and the Scottish Police.

Professor William J. Buchanan
Edinburgh Napier University
3 August 2011