

IN THE MATTER OF THE LEVESON INQUIRY

WITNESS STATEMENT OF GRAHAM CLULEY
SENIOR TECHNOLOGY CONSULTANT, SOPHOS LTD

1. I make this witness statement in reply to a letter of 30 January 2012 addressed to me from the Senior Assistant Solicitor to Lord Justice Leveson's inquiry into the culture, practices and ethics of the Press ("the Inquiry").
2. I am Graham Cluley and I am the Senior technology consultant at Sophos Ltd, a global computer security firm which specialises in protecting businesses against the threat of malware, spam, hacking, data loss and other threats. I have held the position since May 1999, having previously been employed by computer firms McAfee (1998-1999) and S&S International (later known as Dr Solomon's Software) between 1992 and 1998.
3. I have won numerous awards for my work, including "Best Security Blogger" from SC Magazine in 2011, "Most Educational Security Blog" at the RSA Security Bloggers Awards in 2011, "Twitter user of the year" at the Computer Weekly Awards in 2009 and 2010, and "Best IT Security blog" at the same awards in 2009 and 2010. In April 2011, I was inducted into the Infosec Europe Hall of Fame.
4. My role at Sophos is to lead the company's coverage of computer security matters, writing (on our "Naked Security" blog) about computer security news and advice, and being the company's primary spokesperson when appearing in the media discussing infosec issues. I also advise internally on what stories matter, and how they should be presented.
5. Although my current job is largely one of communications, my background is as a software engineer - having written computer anti-virus software early in my career.
6. I do not have personnel management or budget responsibilities, and currently report to the Head of Brand Awareness at Sophos.

What material your blog "Naked Security" publishes, and why.

7. "Naked Security" devotes itself to sharing news, opinion, advice and research on computer security matters. We try to present sometimes complicated, technical security news in a manner which a typical computer user can understand - for instance, how to prevent their email account from being hacked.
8. We largely avoid explicitly promoting the security products that Sophos develops in our articles, preferring to educate users about the risks and methods to avoid threats instead. We believe that publishing interesting, relevant articles will help raise the brand

awareness of our company and hopefully - at some point in the future - result in more sales.

9. In a typical month, "Naked Security" has approximately 800,000 unique readers and receives on average 1.5 million page views each month.
10. It should be noted that although I am a primary contributor to "Naked Security", I am not the site's only writer. We have a team of people - some of whom are security professionals, and others with a journalistic background - who contribute to the site's content.

Where are your servers located?

11. "Naked Security" runs on the WordPress VIP platform, managed by Automattic. WordPress uses hundreds of servers located in several separate data centres in different parts of the USA.

Do you consider the UK courts to have jurisdiction over the way in which your website is operated in the UK, and how far does this jurisdiction extend?

12. Yes – although the Naked Security blog is global. It is not entirely clear to me how far this jurisdiction extends particularly given that many of our contributors are overseas and our servers are located in the US. For example, an individual who is referred to in Naked Security who is resident in another country could bring a claim against us in that country or in the UK and part of that decision would be based around his or her view of the chances of success in the respective courts. Laws around privacy, data protection, defamation and contempt all apply to what we do.

How you source stories (there is no need to name individuals) and where you consider the responsibility for checking sources of information to lie, with you, or with the person who has provided you with the information.

13. Typically there are three main sources for the stories we write on "Naked Security". Firstly, and most importantly, the source will be internal. Sophos's global network of threat research centres discovers new threats on the net, and shares information with the Naked Security blog. Additionally, we will publish articles covering news stories that have broken in other media - for instance, in the national or IT press. In these cases, we typically will link to the sources' report. Finally, we receive news tips from our readers, asking us to investigate issues which they believe to be of interest to us. For instance, a scam spreading rapidly across Facebook. Wherever possible, we confirm the details of the story that we are planning to publish, and look for other independent sources. It should be noted that most of the stories we write about do not feature individuals at their centre, but rather revolve around technological issues or IT companies.

The extent to which you are aware of the sources of information which make up the central items featured on your blog

14. I feel very aware of most of the sources of content on "Naked Security". There are articles written by other contributors where I will have been less involved in the creation of the content, and would not necessarily be aware of where its information was sourced from.

The extent to which you consider that ethics can and should play a role in the blogosphere, and what you consider 'ethics' to mean in this context.

15. In my personal opinion, ethics must play an important role in blogging. When blogs have large readerships they have the ability to spread news very quickly, in a similar fashion to established news outlets, and unless bloggers act appropriately and ethically there is the risk that incorrect news and rumours can be spread amongst the internet population as if it were fact. We must report accurately and, unless we are expressing our own opinions on a matter about computer security, then the piece should be balanced.
16. At Naked Security we make no secret of the fact that we are employed by a computer security company, and that occasionally (although rarely) we might mention or link to its products. Transparency is important, and earns you trust amongst your readers. For the same reason, we approve comments on our blog even if they are critical of our articles.

Do you have any policy which relates to complaints about articles or web pages which are libelous, defamatory or considered to be an invasion of privacy? If not, do you have any relevant practices? Do you ever remove availability to such pages on that basis? The inquiry would be grateful for some examples of this (anonymised if necessary). Please provide copies of any policies.

17. Each article on our blog includes a link to a form where readers can contact the team of writers, including its editor, and provide us with private feedback. We have received a small number of editorial complaints about our stories via this method and have, where appropriate published updates, clarifications and/or apologies for any errors that may have been posted.
18. In addition, each story can be publicly commented on. Comments are pre-moderated, but we have a policy of approving comments - regardless if they are critical of the blog or not - providing we believe them to be non-malicious and relevant to the conversation.
19. On one occasion we received a complaint from a French gentleman whose name was included in a screenshot of a Facebook scam, and - unlike our standard practice - it had mistakenly not been obscured. As the man had no connection with the scam, and was just an innocent party, we replaced the image at the earliest opportunity once it had been brought to our attention, and we published an update - at the man's request - making clear that he was not involved.

Do you consider yourself to be regulated and if so, how and/or by whom?

20. Personally, I consider myself to be regulated by my bosses at Sophos, the law and my personal sense of ethics.

The inquiry would also welcome your views on the extent to which the content of websites, and the manner in which you operate, can be regulated by a domestic system of regulation.

21. It's not clear to me how that would operate practically, or what the relevance would be for a site that devotes itself to discussing computer security rather than celebrity tittle-tattle.

Do you consider that victims of "bad blogging" should be able to seek redress?

22. Yes. No one deserves to have falsehoods written about them, without an appropriate right of reply and the opportunity to set the record straight.

Does/can blogging act as a check on bad journalism?

23. Certainly. Blogging is effectively journalism by citizens, and there are opportunities for citizens to call into question bad journalism. But equally, good journalism can work as a check on bad journalism.

Anything else which you consider will assist the Chairman to arrive at considered conclusions on any aspect of the Terms of Reference.

24. I would be very happy to discuss what can and cannot be done by malware, and the methods which criminals can use to hack into email accounts and spy on the data on other computers.

I confirm that the contents of this statement are true



Signed

8 February 2012

Dated