



ALTERNATIVE LAW FORUM

122/4 Infantry Road, Opposite Infantry Wedding Hall
Bangalore 560 001. Ph: (+91) 80 2286 8757, 2286 5757, 4157 3784
website: <http://www.altlawforum.org>

BY EMAIL

Flash Network Ltd

7, Sapir Road, P.O.Box 12624, Herzlia 4685211, ISRAEL

c/o Solicis Lex

A Wing, 6th Floor, Knox Plaza, Behind Inorbit Mall, Next to Hometel Hotel, Off Link Road, Malad (w), Mumbai 400 062

Dear Sir/Madam

Ref. No.: VD/AM-001-ISL

I am writing to you on the instructions of my client Mr. Thejesh GN who has received a legal notice sent by you dated 8th June 2015. In your notice you have inter alia averred that my client has violated the copyright of your client Flash Network Ltd.

We deny this contention and bring to your attention the following facts and principles in law

1. My client is a reputed software developer for the past twelve years. He is also a reputed blogger and maintains a popular website <http://thej.in> which is utilized by numerous users. He is also a part of various free software communities and has been involved in research, education and creating awareness about issues related to the internet over the years
2. My client owns an Airtel Postpaid with 3G connection. On the 3rd of June 2015, my client found his website to be very slow on the 3G connection. He proceeded to first check his broadband connection which turned out

to be functioning perfectly, and he then checked the site again on his mobile and it was unusually slow.

3. Being an experienced web developer, my client proceeded to debug his website by first checking the source code of his website <http://thej.in> on his mobile. He discovered to his astonishment an unusual and unauthorized piece of code including a script called **Anchor.js** loaded from <http://223.224.131.144/scripts/Anchor.js>
4. Working on the assumption that someone was trying to hack his website or insert malicious software into it, he examined the source code of his website <http://thej.in> but did not find anything wrong with it.
5. He then proceeded, as any software professional would, to examine the inserted script and understand what exactly it was doing. This script **Anchor.js** was exactly three (3) long lines of code consisting of unreadable code. My client re-organized the code to make it readable and called it **Anchor_beautified.js** which then became a page full of code. Examining the code, my client realized that the inserted javascript was embedding an iframe into <http://thej.in> and responsible for slowing down his website
6. He discovered that the malicious Anchor.js code was inserting an iframe from the source <http://223.224.131.144/l8/Layer8Servlet>
7. He proceeded to take screen screenshots of the website showing javascript embedded

thej_in_screenshot_from_2015-06-03_18:49:39.png

thej_in_screenshot_from_2015-06-03_19:01:00.png

8. After this, suspecting that the website belonged to Airtel, he checked who owned the IP address **223.224.131.144** and confirmed that it was indeed an Airtel owned IP address. He then took screenshots of the same to document the details as evidence of violation of privacy and for deficiency of service
9. He then checked the web page <http://223.224.131.144> and took a screenshot of the same and called it **flashnetworks.png**
10. In order to highlight the malicious manner in which this code had been inserted unlawfully into his website, and to educate and inform the general public about it, he proceeded to publish his findings including all the screen shots on GitHub. This is a common practice for anyone

involved with scholarly research on breach of security issues on the internet, and it is generally understood that one solicits advice, further research, corroboration and refutation by publishing the research and asking for comments or amendments.

11. It is also commonly accepted that whenever one encounters any inserted scripts, viruses or spyware, you publish them as supporting document and evidence so other researchers can review your investigation by looking into it.
12. My client has merely followed accepted industry protocol by publishing the necessary lines of code that was inserted into his browser and website, along with the modified version of the same.
13. He published his findings on GitHub which is a collaborative platform for developers. Github is also a publishing platform and every code and document on GitHub gets a Digital Object Identifiers (DOI) [<https://guides.github.com/activities/citable-code/>] which is used for citation. Software developers who are involved with the observation, study or testing of the functioning of a computer programme in order to determine the ideas and principles which underline any elements of the programme commonly publish on Github
14. GitHub is also a common platform to publish academic and scientific science research projects (<https://github.com/blog/1840-improving-github-for-science>) as well as raising important policy questions concerning the rights of citizens online
15. As is evident from the sequence of events above my client has not indulged in any activity which would be deemed an infringement of copyright, and has instead exercised his right in accordance with Copyright law in India. Sec. 52(1)(ac) provides for a fair dealing with a computer program for “the observation, study or test of functioning of the computer programme in order to determine the ideas and principles which underline any elements of the programme while performing such acts necessary for the functions for which the computer programme was supplied”
16. Furthermore his publication of his findings via screen grabs constitute a fair dealing with a work for the purposes of criticism and review, and for the purposes of reporting as laid down in Sec. 52(1)(a)(1)
17. My client is shocked and outraged by the demands made by your client. The unlawful insertion of code by your client into my clients source code amounts to a violation of the rights of my client, including but not limited to a violation of his privacy, an attempt to unlawfully access and hinder the operation of his website and a violation of the right to integrity of the work of my client.

18. The effect if your client's actions have resulted in misleading visitors to my client's website and its functionality thereby substantively affecting the reputation and goodwill that my client has earned through years of expertise and service.

Under the circumstances my clients refuse any liability averred by you, and on the contrary makes the following counter claims and demands.

- A. That your client offer an unconditional apology for attempting to insert a malicious piece of code into my client's website which has affected the functionality of the same as well as lowering the reputation of my client
- B. That you client offer an unconditional apology for violating the privacy of my client

Rather than accepting the legal and moral responsibility for inserting malicious code that compromises the security and privacy of consumers, your client has attempted to use a 'cease and desist notice' to intimidate and silence my client and prevent an open discussion on an issue of immense public interest.

My client reserves the right to initiative civil and criminal proceedings against your client

For Alternative Law Forum



Lawrence Liang

Cc:

1. THE COMMISSIONER OF POLICE, Near Infantry Road, Vasanth Nagar, Bangalore, Karnataka. Email: ksdgp@bgl.vsnl.net.in
2. ADDITIONAL DIRECTOR GENERAL OF POLICE (E.O.), CID, BANGALORE. Cyber Crime Police Station, CID Annexe Building, Carlton House, # 1, Palace Road, Bangalore - 560001 +91- 080- 22094498, +91- 080- 22094564, +91- 080- 22942475, +91- 080- 22943050 Email: cybercrimeps@ksp.gov.in

