

April 19, 2013

Attn: Copyright Agent
Stack Exchange Inc.
110 William St, 28th Floor
New York, NY 10038
Email: dmca@stackexchange.com; team@stackexchange.com

Delivery by Courier and Email

RE: DMCA Notice – Notice of False/Misleading/Defamatory Statements

To Whom It May Concern,

My name is Michael Bartz, and I am Senior Corporate Counsel for CipherCloud, Inc. On behalf of CipherCloud, I am providing notice in this letter that a question/answer posting on a website hosted by Stack Exchange, Inc. (<http://crypto.stackexchange.com/questions/3645/how-is-ciphercloud-doing-homomorphic-encryption>) (the "Webpage") includes repeated infringements of CipherCloud intellectual property, including copyright and trademark. In addition to the DMCA Notice, I am providing samples of false, misleading and defamatory statements made by Subscribers on the Webpage. Both activities are violations of law and Stack Exchange's Terms of Service.

DMCA NOTICE - COPYRIGHT INFRINGEMENT

VIOLATION I

The original image, to which CipherCloud owns the exclusive copyright and includes a CipherCloud trademark, is a screen capture from a slide deck produced and presented by CipherCloud's CEO for the 2011 Defense Science Board Task Force on Cyber-Security and Reliability in a Digital Cloud. Images from the original slide deck are attached to this letter. Specifically, note the second image attached to the end of this letter, which is slide four (4) from the slide deck.

The unauthorized and infringing copy of that image is in a post from CodesInChaos (originally posted 25.August.2012 at 15:31 and edited 25.August.2012 at 15:50). The image is found on the Webpage and is hosted through Stack Exchange's account with Imgur LLC at:

<http://i.stack.imgur.com/xJ6V8.png>

VIOLATION II

The original image, to which CipherCloud owns the exclusive copyright, is a screen capture that can be found at the 2:30 mark of the following video:

<http://pages.ciphercloud.com/AnyAppfiveminutesdemo.html?alild=1>

The unauthorized and infringing copy of that image is in a post from Sid (originally posted 25.August.2012 at 23:12 and edited 13.March.2013 at 1624). The image is found on the Webpage and is hosted through Stack Exchange's account with Imgur LLC at:

<http://i.stack.imgur.com/h7ntP.jpg>

VIOLATION III

The original image, to which CipherCloud owns the exclusive copyright, is a screen capture that can be found at the 2:53 mark of the following video:

<http://pages.ciphercloud.com/AnyAppfiveminutesdemo.html?alild=1>

The unauthorized and infringing copy of that image is linked in a post from adrenalion (originally posted 18.March.2013 at 1638). In the post, adrenalion even states that they "...snapped a copy of one screen after the response from John is entered and encrypted, and have attached an image below (apologies for the crude

highlighting)...” The link to the image is found on the Webpage and is hosted through Stack Exchange’s account with Imgur LLC at:

<http://i.stack.imgur.com/oBXZJ.jpg>

This letter is official notification under Section 512(c) of the Digital Millennium Copyright Act (“DMCA”), and I seek the removal of the aforementioned infringing material from your servers. Please also be advised that law requires you, as a service provider, to remove or disable access to the infringing materials upon receiving this notice. Under US law a service provider, such as yourself, enjoys immunity from a copyright lawsuit provided that you act with deliberate speed to investigate and rectify ongoing copyright infringement.

I am providing this notice in good faith and with the reasonable belief that use of the image in the manner complained of is not authorized by CipherCloud, its agent(s) or by law. Under penalty of perjury I certify that the information contained in the notification is both true and accurate, and I have the authority to act on behalf of the owner of the copyright involved.

STACK EXCHANGE TERMS OF SERVICE - FALSE AND MISLEADING STATEMENT

The postings from CodesInChaos, adrenalion (including their original account as AdrenaLion), Sid and D.W. all include admissions that the individual offering an “answer” does not know the facts of CipherCloud functionality. Some examples from the Subscriber’s own postings include:

- (1) “I’m not sure...”
- (2) “I don’t even think...”
- (3) “I don’t know how...”
- (4) “I have not had time to fully explore this...”

Following these admissions, the Subscribers then make claims of fact that are false, misleading or libelous. We do recognize the purpose of some Subscribers is to defame CipherCloud while purporting to offer crypto information. For example, your Subscriber Sid is affiliated with a CipherCloud competitor as CEO of CipherDB (<http://www.linkedin.com/in/sidshetye>).

Beyond incorporating defamatory statements, such as “snake oil” or “cost with no benefit” as just two examples, the Subscribers make repeated statements purported as fact that can be ascertained as false by viewing publicly available information on CipherCloud’s website (<http://www.ciphercloud.com/>). Such false, misleading and defaming statements include the following sample:

- (1) “The scheme is deterministic and format preserving.”
 - CipherCloud’s product is NOT deterministic.
- (2) “If the same string gets encrypted in different places, an attacker can see that the same string was used in both places.”
 - Again, CipherCloud’s product is NOT deterministic.
- (3) “To make this possible, you must ensure that the same string gets encrypted the same way every time.”
 - This is a false statement about CipherCloud functionality. And again, CipherCloud’s product is NOT deterministic.
- (4) “As CodesInChaos suggested in an earlier answer, this makes the solution extremely vulnerable to frequency-analysis attacks.”
 - The referenced scheme does NOT represent CipherCloud functionality. In fact, CipherCloud has patent pending mechanisms to defeat frequency-analysis attacks.
- (5) “This probably explains why they do not have, and are not even in process to obtain, FIPS 140-2 validation, which pertains to the proper implementation of an approved algorithm.”
 - This statement is patently false. CipherCloud is in process for FIPS 104-2 certification as can be ascertained on the publicly available NIST website.
- (6) “Would you entrust your data to what amounts to XOR?”
 - XOR is only one of the schemes CipherCloud offers, but this statement from AdrenaLion is part of an assertion that it is CipherCloud’s only offering.

-
- (7) "Basically they end up with a 1:1 mapping of lower case words."
- The statement is patently false. Sid implies that what was perceived from a public demo is CipherCloud's product offering. CipherCloud does not incorporate 1:1 mapping.
- (8) "There is no security. AES is misleading/wrong (ECB + 0/constant padding + 0/constant IV => simple 1:1 mapping => why don't you just rotate the bits and call it a day!)"
- CipherCloud does not use ECB, constant IV or 1:1 mapping. Even more concerning is the statement that CipherCloud offer "no security" in its product.
- (9) "Vendor lockin - I don't know if they supply migration tools because if you one day decide to upgrade to real security from their "secure" offering, you can't. Because their box/gateway is the only one that would know these 1:1 mappings. Unless you want to formalize hacking yourself as the official upgrade and data extraction path."
- The statement is simply false, and Sid even admits "I don't know" before going into all of the false statements.
- (10) "What Ciphercloud appears to be doing is not random, therefore it is not truly encryption, and certainly not homomorphic encryption."
- CipherCloud's products ARE based on patented pending randomization. Again, this is a patently false statement intended to defame CipherCloud and CipherCloud products.

The dissemination of false and misleading statements subjects parties, among other things, to claims as a violation of the Lanham Act §43(a) [15 U.S.C. §1125] and California Business and Professions Code §17200 et seq. for unfair competition by a competitor. Furthermore, posting such statements is a violation of CAL. CIV. CODE § 43 as defamation. I also note that posting statements that are libelous, defamatory or violate the law is a violation of Section 3 in Stack Exchange's Terms of Service.

Please be advised that CipherCloud is taking this matter very seriously. CipherCloud demands that Stack Exchange act with deliberate speed to remove the Webpage and notify the Subscribers of their violations of Stack Exchange's Terms of Service. CipherCloud further requests that you respond to this letter within ten (10) days and provide written assurances that you will take all steps necessary to correct the violations of law and CipherCloud intellectual property rights.

By this letter, CipherCloud reserves all of its rights and claims against Stack Exchange. Nothing in this letter shall be deemed a waiver of any kind by CipherCloud. You are now on notice of the possibility of formal legal proceedings regarding this matter, and are therefore required to preserve all documents pertaining to this matter, whether such documents exist in electronic form or hard copy.

We look forward to hearing from you or your counsel concerning this matter. Should anyone from Stack Exchange wish to discuss this with me, please contact me directly at:

Attn: Michael Bartz
Senior Corporate Counsel
CipherCloud, Inc.
99 Almaden Blvd, Suite 500
San Jose, CA 95113
415.363.6475 (phone)
bartz@ciphercloud.com

Thank you in advance for your prompt attention to this matter.

Sincerely,



Michael A. Bartz, JD

attachment



Cloud Data Protection

Pravin Kothari

Founder & CEO, CISA, CISSP
Previously,
Founder & CTO, Agiliance (IT-GRC)
Co-Founder & VP Engineering, ArcSight

Defense Science Board Task Force on
Cyber-Security and Reliability in a Digital Cloud
July 13, 2011

Configuration
Console



Record
as seen by
"authorized users"



Record
as seen by
"Unauthorized Users"



Field Label	Type	Tokenizer
Last Name	String	AES Crypto Encryption
First Name	String	AES Crypto Encryption
Full Name	String	AES Crypto Encryption
Title	String	AES Crypto Encryption
Company	String	AES Crypto Encryption
Street	textarea	AES Crypto Encryption
City	String	AES Crypto Encryption
State/Province	String	AES Crypto Encryption
Zip/Postal Code	String	ID Encryption
Country	String	ID Encryption
Phone	phone	Telephone Number Encryption
Mobile Phone	phone	Telephone Number Encryption
Fax	phone	Telephone Number Encryption

Lead
Mr. Calvin Jefferson

Lead Detail

Lead Owner: John Smith (Change)

Name: Mr. Calvin Jefferson
Company: Albarista
Title: Mr.

Lead Source: Purchased List
Industry: Government
Annual Revenue: \$91,000,000

Address: 5224 Dolor Avenue
Frandor, Vermont 32127
Fakland Islands (Stateless)

Phone: (393) 2441254
Mobile: (593) 4445321
Fax: (748) 5137355

Lead
Mr. TPF Uovycf Hjmuucctc TSF

John Smith (Change)

Mr. TPF Uovycf TSP TPF Hjmuucctc TSP
TPF Uovycf TSP
TPF Uovycf TSP

Purchased List
Government
\$91,000,000

TPF Uovycf TSP TSP TSP
TPF Uovycf TSP Vermont TSP
TPF Uovycf TSP
TPF Uovycf TSP
(393) TPF Uovycf TSP
(593) TPF Uovycf TSP
(748) TPF Uovycf TSP