

Where you did sleep last night?

...Thank you, I already know!

Abhishek Dhingra

*Candidate for M.Sc. In Analysis Design and Management of Information Systems
Information Systems and Innovation Group
Department of Management
London School of Economics*

I know where you were last night. I know the salad was delicious, the look on your face says it all. I wonder why you have to diet; you look absolutely captivating to me whenever you don that black dress. He never deserved to be with you. Just look at the meager £1 tip he could spare for the waitress. I know I swore out loud each time he touched you. And why did you kiss him back? Sheer profanity! I know I bled when I broke the window pane on my fist. I know. I know it all. I'm your Facebook stalker!

Potential victims: over 60 million

Criminal opportunities: over 1.7 billion

A picture is worth a thousand words, or should I say, a thousand wounds! Each one of those 1.7 billion uploaded photographs is capable of shattering trust, annihilating relationships and wrecking lives. Each one of those 60 million active users, mere victims! I know. I know it all. I'm the one, who shall substantiate in the next 2800 words that Facebook albums are neither private nor secure.

I can see you, beh-bie!

Facebook.com is a minefield for its users. One faux pas and an entire private life could blow up and disperse into the vast and resounding expanse of the Internet. Since its inception in 2004, numerous questions have been raised about the security of data and the privacy of users. Due credit should be given to Mark Zuckerberg and his team for covering up for 'technical glitches' and reassuring the users of security after applying quick plasters to the 'technical marvel'- a large poster-board where anyone with the slightest knowledge of PHP can paint and patch up their own applications. Due credit should be given to the users for believing each word he ever said, and for their loyalty to what has the potential of being the 22nd largest nation by population, displacing the UK in the list.

Let me get down to decimating the certitude and establishing the facts. This is not an attempt to ravage the medium itself, but a cry for cognizance and the exercise of discretion. I am not a vandal; I am an antagonist of blind faith. I urge you, the reader, to look beyond the credence and invite you to try the following as I state them. A word of caution, though. Facebook is not a mere medium anymore; it is an adoration that has grown to a worldwide size that can outnumber the Protestants in North America over the next 5 years. What follows here may be termed as blasphemy, though I prefer to call it apocalypse.

Security on Facebook albums is a mere dance of obscurity. It

works on the premise that if you cannot type it, you cannot see it. Being the sceptic that I am, I argue that the premise is flawed. Anything that is on Facebook is public for anyone to see and use, if they can guess the URL right. A very obvious question arises from the last statement.

How can one guess the right URL?

The answer to that question is as trivial as the English alphabet is to a first grader in Britain. Let me try and answer that with another question.

How would you 'guess' the URL of the website of the Ministry of Health in India?

If you said, "Google it", rest assured that you 'guessed' the answer right. Google the following and you are in for the first shock.

Allinurl: "facebook.com" "album.php"

A mere click on the "repeat the search with the omitted results included" link at the bottom of the search results and Google lists out all the URLs that have the keywords "facebook.com" and "album.php". Replace the keyword "album.php" with "photo.php" in the search query and Google, as an obedient dog, fetches the URLs to user photographs on Facebook. These are not public albums, thus **not all** clicks on these links would lead us to a photograph. Not yet, but by the end of this section, I hope to be able to join the dots and spot both the Timon and the Pumba of the issue.

I hate to get technical, but hey, who in their right mind lets go of an opportunity to prove their ingeniousness? If you still secretly wonder what makes an electric toaster smart enough to pop the toast up when it is done, maybe you should skip to the next section.

Facebook assigns a unique URL to each album and photograph. This URL is visible to only the owner of the album/photograph and exists so that the album/photograph may be shared if the owner intends to. *However, if the owner does not intend to share the albums/photographs, is this URL secure?* The answer is **no**. The URL is merely **obscure**. Using this URL the album/photograph can be globally accessed by anyone. Access is instantly granted independent of the privacy settings on the owner's profile. The most ominous part about these URLs is that the viewer does not even need to be a Facebook user to be able to access these. The implications are unmistakable. There is no record of all who can witness your private life in all its *stark nakedness*. This global access URL is the *only* stylus one needs to join the dots and make a picture worth looking at.

Let us take a closer look at the URL itself. The following is a sample global access URL. Click on it to say a quick personal hello to the overlord of Facebook himself— Mark Zuckerberg, with his girlfriend, Pricilla Chan, at a photo shoot for *BusinessWeek*. If I were you, I would mouth a quick swear instead, but that is just me! Where did I find the URL? I found it exactly where I found the URL to the Ministry of Health in India.

<http://harvard.facebook.com/photo.php?pid=30054437&id=4&l=ae012>



Exhibit 1: Mark Zuckerberg and Pricilla Chan

Each of these URLs is made up of parameters that follow the question mark symbol (?) and are separated by the ampersand symbol (&). A global access URL would consist of three such parameters. *What are these parameters?* Facebook identifies these parameters as the following.

1. **id** – A unique 128-bit number that represents a user's Facebook profile. This unique number is readily made available to anyone who runs a Facebook search for a particular user, through the link to their profile on search results listing page. Easier still, running a Google search for a particular name, and a bit of luck, would fetch the URL of the public listing of that user's profile. This URL contains the unique id. If you happened to act smart and set your privacy settings to block Google from indexing your profile, rest assured some 'cool dude' on that friends list of yours wouldn't have been that smart. If Google can index them, you can be reached.
2. **aid/pid** – Another unique 128-bit number representing an album or photograph in the Facebook database. Remember the "allinurl" query results from Google? That is where you nail this number down.
3. **l** – This is the key to all locks— the global access parameter. I wonder why Facebook recognizes it as 'l' and not 'access' or 'key' itself. Maybe, it is just a part of 'Facebook's security through obscurity' plan. A 5-digit hexadecimal number. Hold on to that thought for a minute. This would have magnified ramifications as we progress.

Having observed the above mentioned trends and with some knowledge and experience of information security on the Internet, it was unmistakable that Facebook albums could be broken into. I decided to be astute about the issue and ask the experts before sounding the panic alarm. My research led me to interview Priyank Thakur and Narendranath Tangudu, who have spent years of their career working as Security Specialists at the IBM Software Labs. Their words testified that there was an actual fire behind the smoke.

In the information security domain, we are always threatened by one basic premise.

"If it was generated by an automated code using a particular logic, it can always be generated again by another auto-

mated code if the governing logic can be reverse engineered."

The idea behind securing an application is either to ensure manual intervention (as in the case of a *captcha*) or to make reverse engineering on an automated result incredibly time consuming and uneconomical. Our friend here – the global access parameter 'l', subscribes to neither of the two. Even for an amateur, detecting the logic behind the generation of a 5-digit number is neither infeasible nor impractical.

Priyank said, "Reverse engineering to fabricate the logic of the global access parameter is a three step process.

1. Perform a few sample registrations.
2. Get a set of Album IDs and URLs.
3. Crack the logic using logic sniffing based on a few parameters like timestamps and utilizing methods in the line of neural networks."

He went on to say that even a dump of URLs containing the parameters pooled from a proxy server or a public Internet access café can provide the sample data set for sniffing the logic. The only challenge he identified in the process was the lack of information on the inputs to the automated parameter generation code, which he said, could be guessed to some extent. A preliminary analysis later, the probable inputs to the parameter generator were guessed to be the owner ID, the album/photograph ID, and time stamp/date of the creation of the album or a combination of these. Using neural network based transformation/data predictors on the web one can sniff this logic for fabrication with fair accuracy.

What if the logic for generation of this parameter is actually obscure? Let us talk about the possibility of a brute force attack. Since it is only a 5-digit hexadecimal number, the possible values it can have are exactly 983,039. Priyank examines the issue and testifies that the possibility of a brute force attack is considerably high given the small range. He says, "A simple Web-Reaper can be customized to pick up the values of global access parameter from a file to download the entire data from the URLs generated. This would not take much effort, time or finances and the only challenge could be an intrusion detection system at the website."

The Larger Picture

If you happened to get through the entire technical parlance of the issue, it is now time to arrange all the larger pieces of the puzzle. With a recently updated value tag of \$15 billion and a trust base of over 60 million, is Facebook selling nothing but an illusion of privacy? Priyank argues, "Facebook's approach for albums cannot be deemed as unsecure. There is a possibility of breach of privacy in case an amateur hacker chooses to hack some particular albums, but in case of intrusion, only mass download of pictures will not be taken as a breach considering the bulk of data". Sorry Priyank, I beg to differ. In December 2005, Jones and Soltren took up the task of a mass download of user profiles from Facebook and published a paper on the dismaying state of affairs. The following are extracts from their paper. The findings clearly exhibit that Facebook is nothing but a mass massacre of users.

"It served as a proof of concept, to demonstrate that it is possible for an individual to automatically gather large amounts of data from Facebook. The collection of data was not entirely trivial, but we were able to produce the scripts necessary to do so within 48 hours. The final application we used to download profiles was a short (five line!) BASH shell script. We ran this script four times: once for Harvard, MIT, the University of Oklahoma (OU), and New York University (NYU)."

Success Rates In Downloading Profiles

School	Number Profiles	Number Downloaded	Percentage
MIT	10063	8021	79.71%
Harvard	25759	17704	66.16%
Oklahoma U.	28201	24695	70.54%
NYU	32250	24695	77.41%
Total	97273	70311	72.28%

Exhibit 2: Success Rates of Mass Data Download²

Narendranath has a more entrepreneurial take on the issue. He suggests, "It is only the photographs of the users that can be accessed using the logic discussed. They are used only on a view basis, not on an edit basis. The information is not sensitive in nature, at least not to Facebook. Social networking has a governing principle— anything put on there is not private and is accessible to all. Facebook is a business too. It is governed by the same principle". How reassuring! Priyank explains that these flaws could have three-fold ramifications for Facebook— legal, loss of business and loss of credibility. My question is more sinister. *What are the users hell-bent on compromising?*

Heads and Tales

"We could all donate a dollar each and raise millions to hire an assassin to kill the US president and replace him with a monkey."

In March 2005, this cry of a University of Oklahoma freshman was met with US Secret Service's intent of framing him.

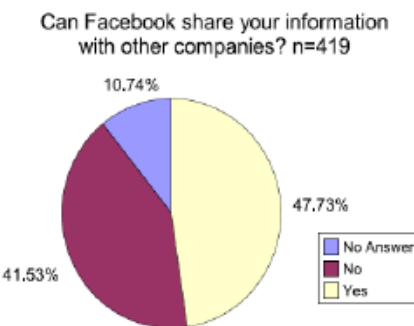


Exhibit 3: For ignorant users: Facebook legally shares information

all information published on the site should be presumed available to the general public, school administrators included. Legal experts agree that Facebook can be legally used in criminal or other investigations.

I don't know if American Facebookers considered him to be a threat or a saviour, but I do know that Facebook has been increasingly used as source of evidence for disciplinary action and law enforcement. Despite Facebook's Terms of Use, their spokespeople clearly state that

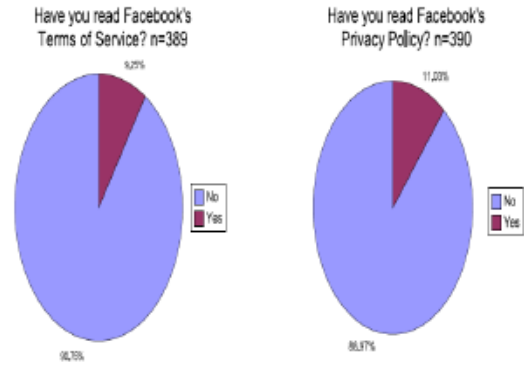


Exhibit 4: Users never read the fine print

In February 2006, a Miami Facebooker was arrested for creating panic by having the police sketch of a rapist accused as his profile picture. April 2006 saw a University of Dayton student being fined for \$10,000 as damages caused by "Lowesfest", the Facebook invitation that was sent by him. He never attended the festival himself. In October 2006, a Southern Illinois university student faced expulsion for Facebooking his sexual escapades with his girlfriend, who "never thought Facebook could cause real-life problems". In February 2007, Alvino was traced using Facebook and charged for a hit-and-run. In the light of the Virginia Tech shootings, a SUNY student was sent to psychiatric remand since he had vaguely threatening photographs on Facebook.

Even though cyberstalking has been recognized as a growing menace and states are finding it increasingly hard to keep the laws in shape to deal with it, most incidents often go unreported.

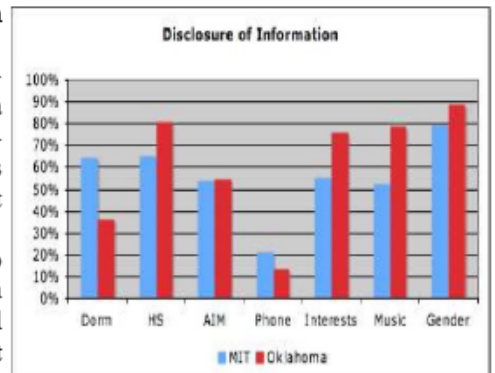


Exhibit 5: Overexposed??

Statistics reveal that women on social networking websites are thrice as susceptible to stalking as they are to rape, with each incident lasting 1.8 years on an average. With Facebook, you're the next potential Monica Seles.

Do you ever friend people whom you have never met in person? n=383

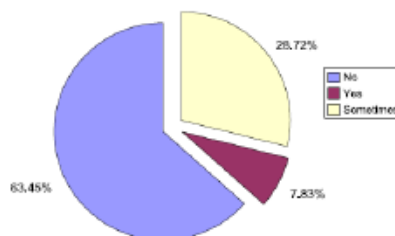


Exhibit 6: Overfriendly or Actively Social??

Julie was chosen by her cyberstalker when she bought a DVD from his shop in LA. Digging her up on the Internet, he broke into her house and installed a webcam to stream every second of her bedroom to his live website,

and Internet security, he could never be traced, though the website was taken down. Manish Kathuria became the first criminal of cyberstalking in India, after he had been stalking Ritu Kohli for months.

Another emergent theme from social networking is social pornography. In December 2004, an MMS video of a 15-year old school girl in Delhi performing fellatio on her boyfriend became a rage in India, and online social networking communities helped it spread further, publicly shaming her for life. Similar cases led to a market of 'real porn' as opposed to 'directed porn' and people started sharing videos and links to social porn using social networks. Morphing of images on the web for pornography has been a widely known phenomenon. In a separate incident, a 16-year old Delhi boy was taken into custody for morphing and uploading images of his school teachers and peers onto a pornographic website. Incidents of this nature are countless and Facebook is the most advanced tool to label the girl next door as 'America's Next Porn Star'.

You can check out anytime you like, but you can never leave

This is when I stop talking 'Geek and Latin' and narrating stories that most readers would still audaciously label as 'one-off incidents'. Let us talk numbers. Running the risk of sounding like the blabber of a grumpy old man with gray wildness growing off his scalp, I'll reiterate that *'the problem with this generation is that they'll talk-the-talk but won't walk-the-walk'*.

Satisfaction with Facebook Privacy, by gender

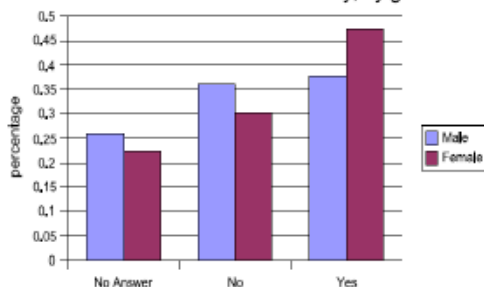


Exhibit 7: Satisfaction with Facebook Privacy From the survey results produced by Jones and Soltren, it became clearly evident that a total of 33.17% people surveyed were sure that they were not satisfied by Facebook's attempts to protect a user's privacy. This figure translated to 41.34% of the survey sample being concerned over their privacy on Facebook.

I decided to take this one step further by surveying a carefully selected sample of 50 male and 50 female college students, who were Facebook regulars. On asking them if they would stop using Facebook albums if it could be proven that all Facebook photographs are globally accessible to absolutely anyone, 84% women said yes, while 52% men said no. The question still stands. How many of these will actually walk-the-walk?

Concerns with Facebook Security, by gender

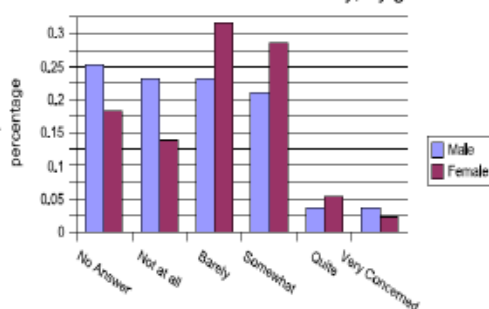


Exhibit 8: Concerns with Facebook Security

"Why would this stop me from 'facebooking'? Not for a minute have I entertained the thought that FB is even remotely secure... I'm just confident that my face will not fit a porn star's body!" - a Masters student at the LSE

The final nail in the coffin. Facebook is stickier than you can imagine. While the website offers users the option to deactivate an account, the servers keep copies of the information in those accounts indefinitely. Nipon Das had to go head-to-head with Facebook's customer service for two months and threaten them with legal action for most of his profile to be erased. Even after that, a reporter was able to find his empty Facebook profile and successfully sent him an e-mail message. Steven Mansou decided to write a blog entry— a detailed account of his frustration— "2504 Steps to closing your Facebook account".

The question is right here and standing tall in our face. Have we been 'facebooked' beyond reason? **I can see I am going blind! Can you see what I see?**

Acknowledgements

I am thankful to **Priyank Thakur** and **Narendranath D. Tangudu**, IT Specialists for Enterprise Application Security at the IBM India Software Labs, for finding the time to be interviewed for the purpose of this article. It was very kind of them to share their knowledge and expertise while analyzing the issue with me. I am also thankful to my dear friend **Merlia Shaukath** for her assistance while carrying out the survey and writing the article.

References

1. The title draws its inspiration from the popular track "Where did you sleep last night" by the grunge metal band Nirvana.
2. The idea of Facebook stalker originated from a YouTube video by the title "Facebook Skit". It is a lively parody of the song "Hero" by Enrique Iglesias and goes like, "I can be your Facebook stalker".
3. The statistics about the user base and the number of uploaded photographs on Facebook.com have been taken from Wikipedia. The story about Zuckerberg reassuring the users after the Facebook beacon protests is also from the same source.
4. The statistics about the population of nations was taken from the US Census Bureau-International Database 2008. <http://www.census.gov/ipc/www/idb/index.html>
5. The world wide religious break up and the number of Protestants was taken from the Worldwide Adherents of All Religions by Six Continental Areas, Mid-1995 database. <http://www.zpub.com/un/pope/relig.html>
6. The idea of the global access parameter in the URL being used for breaking into Facebook albums originated while uploading personal photographs to Facebook albums. Researching the same led me to find more information about Google indexing Facebook profiles at FunnyTechPants. Valleyway also had an article about Facebook im-

- ages being insecure because of the global access parameters.
<http://funnytechpants.blogspot.com/2007/06/facebook-hack-view-non-friends-albums.html>
<http://valleywag.com/345763/facebook-bullies-writers-not-its-engineers-to-keep-data-private>
7. The explanation on URLs and Google was a result of spending a lot of time researching the issue by trial and error. Interviews with Priyank Thakur and Narendranath D. Tangudu, who work as IT Specialists for Enterprise Application Security with IBM India Software Labs, were carried out over E-mail and telephone to testify the logical and technical correctness of the findings. The interview transcript has been attached along with as an appendix.
 8. The valuation of Facebook at \$15 billion was a figure taken from Wired.
www.wired.com/techbiz/startups/news/2007/10/facebook-future
 9. A lot of survey results, graphs, an extract and the result of mass download of Facebook profiles was taken from the paper "Facebook: Threats to Privacy" by Harvey Jones and José Hiram Soltren, December 2005.
 10. The University of Oklahoma story about the US Secret Service and the Facebook post by a guy was taken from Oklahoma University Daily.
http://www.oudaily.com/vnews/display.v/ART/2005/03/08/422db16170829?in_archive=1
 11. Policing using Facebook emerged from the article "Campus police use popular service to hunt criminals, cyberstalkers".
<http://www.californiaaggie.com/media/paper981/news/2006/01/18/Features/Policing.The.Facebook-1476877.shtml?noreferrer&sourcedomain=www.californiaaggie.com>
 12. The story about the Miami Facebooker who got arrested for creating panic was taken from The Miami Student.
<http://www.miamistudent.net/media/paper776/news/2006/02/10/FrontPage/Student.Arrested.For.Inducing.Panic.With.Facebook.Picture-1607555.shtml?noreferrer>
 13. The LowesFest story was taken from The Flyer News.
<http://www.flyernews.com/article.php?section=Opinions&volume=53&issue=39&artnum=03>
 14. The story of the man writing about his sexual escapades was taken from "Students learning dangers of Web 'confession'; Sophomore may be expelled for Facebook page" published in The Record on October 5, 2006.
 15. The hit-and-run story was taken from The Courant.
<http://www.courant.com/news/local/hc-uconnarrests0216.artfeb16.0.4348643.story>
 16. The psychiatric remand story following the Virginia Tech shootings was taken from The Washington Post.
<http://blog.washingtonpost.com/offbeat/2007/04/facebook-k-guns-the-virginia-tec-1.html>
 17. The statistics on cyberstalking were taken from the Stalking Attorney. Other sources that I referred to while researching cyberstalking were Female First, "Is facebook an open invitation for stalkers?" by Matthew Watkins, "Confessions of Facebook stalkers" by Byron Dubow for USA Today and "Facebook: A stalker's dream" by Rosanne Palatucci published in The Heights on April 27, 2004.
<http://www.stalkingattorney.com>
<http://www.femalefirst.co.uk/relationships/Relationships-88.html>
 - http://www.tamu.edu/upd/is_facebook_an_open_invitation.htm
 - http://www.usatoday.com/tech/webguide/internetlife/2007-03-07-facebook-stalking_N.htm
 - <http://media.www.bcheights.com/media/storage/paper144/news/2004/04/27/Features/Column.Facebook.A.Stalker.Dream-671350.shtml>
 18. The cases of Julie and Mrs. Ritu Kohli were found on Rediff.com in an article titled "Every breath you take" by Ruchi Sharma. The Ritu Kohli case was cross checked on Cyber Laws India.
<http://www.rediff.com/search/2001/jan/23cyber.htm>
<http://cyberlaws.net/cyberindia/2CYBER27.htm>
 19. Both cases of Pornography in Delhi were taken from two separate articles in the Times of India.
<http://timesofindia.indiatimes.com/articleshow/1145421.cms>
<http://timesofindia.indiatimes.com/articleshow/409953300.cms>
 20. The following sources were also referred to while examining morphing of digital images on the web for (child) pornography.
<http://www.wtop.com/?nid=25&sid=1351126>
<http://jmw500.blogspot.com/2004/11/morphing-and-child-pornography.html>
 21. I conducted a survey asking a carefully selected sample of 50 male and 50 female college students, who were Facebook regulars, if they would stop using Facebook albums if it was proven that their content on it was globally accessible by anyone. This survey was a one-question survey and was carried out on Facebook itself. The available options were 'yes' and 'no'. The exact survey question has been attached along with as an appendix. The quote from Merlia Shaukath also came as a response to the same survey.
 22. The 'final nail in the coffin' paragraph originates from the article "How Sticky Is Membership on Facebook? Just Try Breaking Free" by Maria Aspan published in The New York Times on February 11, 2008.
http://www.nytimes.com/2008/02/11/technology/11facebook.html?_r=3&pagewanted=1&ei=5087&em&en=dba4aa893be4b0f9&ex=1202878800&oref=login

About the author

In 2005, Abhishek Dhingra graduated amongst the top 2% of his class in India, with distinction grades and a Bachelor of Technology degree in Computer Science and Engineering. Before being accepted for the MSc ADMIS class of 2008 at the London School of Economics, he worked in the role of a Technical Associate at Tech Mahindra Ltd. And a Security Expert/Consultant at IBM Global Services. His education at the LSE has been generously funded by the school. He is now researching the work-lives of IT workers for his dissertation.