

# FACEBOOK FACIAL RECOGNITION



© Copyright August 2011

All Rights Reserved

<http://www.petergehr.com>

Must not be Sold, Distributed or Republished without the Express Permission of the Author

Dear Friends,

The information contained in this report was compiled from research that I originally compiled for my kids.

As a parent, I find myself on constant heightened alert for opportunities that I promptly pass on to my children, family and friends.

In this particular case, I had come across some information that was not necessarily an opportunity, but insights that I wanted my loved ones to be aware of, and to make a decision on for themselves once assimilating the findings.

I'm hoping that you too will find this input useful and directional.

In summary, the object of this report is to:

1. Offer insights into the current privacy settings within Facebook
2. Include comments and quotations from both advocates and administrators
3. Interview with social networking activist Cory Doctorow
4. How to prevent privacy violations on your Facebook account

# Facts You Should Know About Facebook Facial Recognition

The face-off with Facebook is about to step up a notch from the former outrage it caused when your list of Friends, gender, pages you liked, region and networks were made public without your permission.

If this gets your attention, well, things just got a lot more personal than you may know.

Facebook has clandestinely enabled Facial Recognition software to run freely across its Network—and you have not been consulted with or given an option to opt-in.

This may be no cause for concern for some people, but to those who appreciate the right to decide, and the right to choose—read on.

This new feature has been somehow under-reported and is being described by the Social Media giant as an itty bitty little tag for your “suggest photos of me to friends.”

Furthermore, even if you decide to disable this option, Facebook will continue using technology which will connect your image and name whether you like it or not.

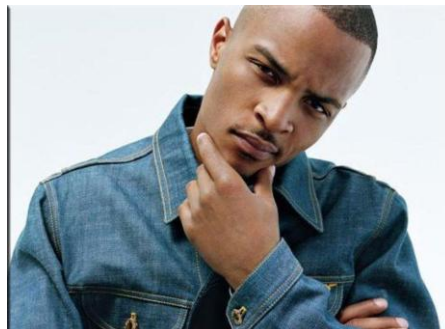


Mark Zuckerberg reportedly has said,

“We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are.”

This is somewhat contrary to his assertion that Facebook operates with privacy at the forefront of its intent.

Let’s get real, if you were asked to “opt-in” to enable Facial Recognition Photo Tags on your Facebook profile, I’m guessing you’d either wait or give it some thought before accepting, right?



Cory Doctorow, noted Social Media activist and writer is quoted as saying that Facebook essentially utilizes, "...very powerful game-like mechanisms to reward. It embodies B.F Skinner's famous thought experiment: the notion of the Skinner box lavish[ing] you with attention from the people that you love in service to a business model that cashes in the precious material of our social lives..."

In other words, the "game" that we play in Social Networking caters to our sense of belonging and our innate desire to socialize with fellow humans, and being that the world is at our fingertips via Facebook (and others such as Twitter, LinkedIn, MySpace, Bebo, Multiply etc.) the ease of exposure to what would otherwise be potential privacy infringements are overlooked due to the "fun" nature of the platform.



Facebook stores an enormous profile photo collection identifying millions of its members into social groups and points of interest, and is such a large collection of data that a leading internet security officer was quoted as saying, "Facebook has the largest collection of identified photos outside of governments. I don't think we know what the ramifications of that will be."

You'd have to ask yourself what the commercial value of that would be, especially since it looks like it will be publically traded later this year, and recently accepted \$450 million from Goldman Sachs, and another \$50 million from a Russian source.

The current valuation of the Facebook empire is a nice piece of pocket change of \$50 billion. Ka-ching!

According to the New York Times, this makes it worth more than eBay, Yahoo and Time Warner.

This sort of cash will allow for development, and the pursuit of acquisitions that it may have in its sites.



I digress.

Let's get back to Facial Recognition.

I read that the senior editor of CSO Online stated, "Many privacy advocates feel Facebook needs to do a better job of educating folks about what the new feature is, what it does, and how to opt in or out. Many also feel a user should always be opted out of new features automatically, and should then have to opt-in themselves."

Just imagine once the sort of data Facebook has in its coffers is made accessible to 3<sup>rd</sup>-parties, Pandora's Box will open and no chance of controlling what that information is used for at that point.

Meddling with privacy settings beyond our control is exactly that—beyond our control, and spamming, scamming, scraping and security holes reveal themselves daily.

Have you noticed an increase in spam on your Facebook lately? It's getting to a point where you can't find your friends amongst all the spammers. It takes regular deletions and edits to keep your FB page clean enough to process your posts, likes and shares.



According to the Wall Street Journal, 3<sup>rd</sup> party apps were "...sending Facebook ID numbers to at least 25 advertising and data firms, several of which build profiles of internet users by tracking their online activities...".

Doesn't it seem weird to you that you're not asked permission or offered options to disable or enable functions that reveal your data and expose your personal privacy affairs?

Of course, our governments already hold a lot of facial database information via passports, drivers licenses, bank accounts, emails, spending habits from your credit cards, etc., and these institutions do not need Facebook for that sort of information, but it's the fragility of a non-Government organization that holds a tremendous pool of information within its servers that may need some attention on our part.

Facebook's Facial Recognition was implemented in the US without any preapproval of opt-in process. It came to the fore once this feature was introduced overseas that it started getting noticed and reported.





A complaint from the executive director of Electronic Privacy Information Centre, Marc Rotenberg, was lodged to the Federal Trade Commission. Rotenberg points out that Facial Recognition in this application raises concerns and “unfair and deceptive trade practices”.

Digital Democracy, Consumer Watchdog and Privacy Rights Clearinghouse have also come to the party asking "the commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to cease collection and use of users' biometric data without their affirmative opt-in consent, require Facebook to give users meaningful control over their personal information, establish appropriate security safeguards, limit the disclosure of user information to third parties, and seek appropriate injunctive and compensatory relief".

It's great to be in touch with buddies, share photos and stories, updates on your holiday, or just saying “Hi” to strangers, but are we okay with losing the ability to decide whether or not we disclose our personal information?



We do what we can to protect our kids online and monitor their activities on the internet by restricting certain sites or completely overwhelming them with house rules and regulations, but then we turn around and lose all control over our own privacy decisions to Facebook?

In a recent statement from the attorney general, George Jepsen, "The lack of an opt-in process for Facebook users is troubling because unknowing consumers may have their photos tagged and matched using facial recognition software without their express consent, potentially exposing them to unwelcome attention and loss of privacy..."



These consumer advocates point out a valid argument that Facial Recognition technology allows Facebook to extort control of user images fully from the user.

We're talking a truck load of photos, in fact, around 60 billion of them. This is a colossal figure compared to the combined 20 billion of PhotoBucket, Flickr and Picasa.

The response from a spokesman for Facebook has said that the company should have "been more clear with people during the roll-out process when this [Facial Recognition] became available to them."

## Cory Doctorow Social Networking Media Activist



The following is a transcript of an interview with Cory Doctorow, writer and social media security activist that I find both informed and thought-provoking.

Although we take lightly the entertainment and social factors related to Facebook, privacy issues are eroding and we are losing our power to decide for ourselves about ourselves.

This is not just a matter for us as individuals, but is a matter that encroaches on our private space, our families, friends, relatives and society as a whole.

This interview expressly addresses the right to privacy and the empowering right to decide for ourselves. We can regain control of our personal matters to public and unsupervised Networks if we choose to.

[Monday 18 April 2011. Guardian.co.uk] *The advice that I would give to parents about their kids using the internet is to realize that you won't be able to supervise your kids' internet use from nose to tail, that your kids will have lots of unsupervised internet use.*

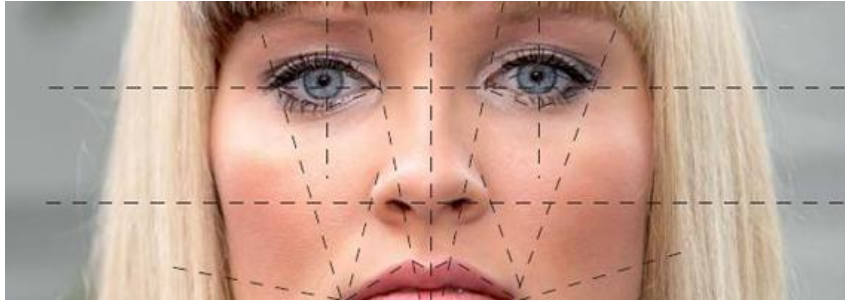
*The only thing you can do to keep them safe in their use of the internet is to instill in them good values and good sense. The way that you do that is by teaching them those things like their privacy is quite important and valuable. The way that you do that is not by spying on them, which is what we do now.*

*We say, "We'll just monitor everything you do on the internet as a means of insuring that you don't do the wrong thing." The way you do it is by teaching them not to be spied on, and that will ripple down.*

*So years before they get to Facebook, if we start teaching them not to haemorrhage personal information when they use networks and when they use mobile phones, and how to take steps to staunch that, then maybe when they get to Facebook, by the time they are enmeshed in Google's data-harvesting mechanisms and so on, they will actually have some sense of why they should take some countermeasures.*

*I think the earliest social networks, the Friendsters and so on, hit on a strategy, really without meaning to, of using negative reinforcements, Skinnerian reinforcement, to get people to disclose more information about their lives, and that each subsequent generation of social network technologies, right up to Facebook, have refined that.*

*The way that they work is that the more you disclose about your personal life, the more the people who matter to you reward you with attention, and that's a really powerful force for encouraging you to go on disclosing information.*



*I don't think that anyone sat down and said, "Hmm that Skinner was on to something. I bet we could create this privacy apocalypse in 15 years if we started building social networks that way." I just think someone hit on a winning strategy and all their competitors ever since have refined it.*

*The EU, on the other hand, is passing data-retention regulations, is increasing the power of the state to wiretap its citizens with any particular suspicion, basically saying, "The good and proper way for the Internet to be run is for Telcoms giants and governments to collaborate on hovering in as much information as they can about the daily lives of individuals who have done nothing wrong and are suspected of nothing." And at the same time they're saying, "But, we expect the private sector to have some privacy policies that have teeth and are meaningful."*

*I think the most powerful mechanism we have for securing the privacy of individuals is for individuals to care about their privacy and to think that it's not a lost cause to do something about their privacy.*

*In order for that to happen, I think states have to stop acting like the Internet is just a playground for sort of extracting data willy-nilly and building dossiers that put the stasi to shame, and start acting like gathering information on the Internet is something that should only happen in the most narrow and closely, judicially supervised circumstances that we know about.*

*Instead of ISPs being required by law to log everything we do and keep those logs forever, we should make ISPs liable if they lose logs, and create financial incentives for ISPs to log as little as possible. [End of interview]*





After reading all this, if you've decided you'd like to disable Facebook from using Facial Recognition on your profile, follow the steps below:

1. Go to your "Account" drop-down menu (top right) click "Privacy Settings."
2. Go to "Sharing on Facebook" and click on "Customize Settings."
3. Go to "Suggest Photos of Me to Friends" under the "Things Others Share" section.
4. Click on "Edit Settings."
5. Click "Disable" in the drop-down to the right.

Thanks for reading, and I hope this information was useful to you.

To your success,



Peter Gehr

<http://www.petergehr.com>

**For more timely and pertinent information  
and free reports visit here:**

<http://www.petergehr.com/index2.html>

<http://www.petergehr.com/index6.html>