



(<http://saintsal.com>)

SAINTSAL

Salim Virani - creating practical ways for founders  
to help each other.

# GET YOUR LOVED ONES OFF FACEBOOK.

29 JAN 2015

*I wrote this for my friends and family, to explain why the latest Facebook privacy policy is really harmful. Maybe it'll help you too. External references -- and steps to get off properly -- at the bottom.*

"Oh yeah, I've been meaning to ask you why you're getting off Facebook," is the

guilty and reluctant question I'm hearing a lot these days. Like we kinda know Facebook is bad, but don't really want to know.

I've been a big Facebook supporter - one of the first users in my social group who championed what a great way it was to stay in touch, way back in 2006. I got my mum and brothers on it, and around 20 other people. I've even taught Facebook marketing in one of the UK's biggest tech education projects, Digital Business Academy. I'm a techie and a marketer -- so I can see the implications -- and until now, they hadn't worried me. I've been pretty dismissive towards people who hesitate with privacy concerns.

Over the holidays, I thought I'd take a few minutes to check on the upcoming privacy policy change, with a cautious "what if" attitude. With our financial and location information on top of everything else, there were some concerning possibilities. Turns out what I suspected already happened 2 years ago! That few minutes turned into a few days of reading. I dismissed a lot of claims that can be explained as technically plausible (*or technically lazy*), based on a bit of investigation, like the excessive Android app permissions. But there was still a lot left over, and I considered those facts with techniques that I know to be standard practice in data-driven marketing.

With this latest privacy change on January 30th, I'm scared.

Facebook has always been slightly worse than all the other tech companies with dodgy privacy records, but now, it's in it's own league. Getting off isn't just necessary to protect yourself, it's necessary to protect your friends and family too. This could be the point of no return -- but it's not too late to take back control. (<https://medium.com/@SaintSal/you-are-our-first-defence-b86ae9a1fff6>)

It's not just what Facebook is saying it'll take from you and do with your

information, it's all the things it's not saying, and doing anyway because of the loopholes they create for themselves in their Terms of Service (<https://www.eff.org/deeplinks/2010/04/facebook-timeline>) and how simply they go back on their word ([https://en.wikipedia.org/wiki/Criticism\\_of\\_Facebook#cite\\_ref-informer\\_33-0](https://en.wikipedia.org/wiki/Criticism_of_Facebook#cite_ref-informer_33-0)). We don't even need to click "I agree" anymore. They just change the privacy policy and by staying on Facebook, you agree. Oopsy!

Facebook doesn't keep any of your data safe or anonymous, no matter how much you lock down your privacy settings. Those are all a decoy. There are very serious privacy breaches, like selling your product endorsement to advertisers (<http://www.forbes.com/sites/anthonykosner/2013/01/21/facebook-is-recycling-your-likes-to-promote-stories-youve-never-seen-to-all-your-friends/>) and politicians (<http://www.zdnet.com/article/is-facebook-damaging-your-reputation-with-sneaky-political-posts/>), tracking everything you read on the internet ([http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1717563](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563)), or using data from your friends to learn private things about you (<http://www.digitaltrends.com/social-media/facebook-snitch-on-friends-that-arent-using-real-names/>) - they have no off switch.

Facebook gives your data to "third-parties" through your use of apps, and then say that's you doing it, not them. Everytime you use an app, you're allowing Facebook to escape it's own privacy policy with you and with your friends. It's like when my brother used to make me punch myself and ask, "why are you punching yourself?" Then he'd tell my mum it wasn't his fault.

As I dug in, I discovered all the spying Facebook does -- which I double-checked with articles from big reputable news sources and academic studies that were heavily scrutinised. It sounds nuts when you put it all together!

- They have and continue to create false endorsements (<http://www.forbes.com/sites/anthonykosner/2013/01/21/facebook-is-recycling-your-likes-to-promote-stories-youve-never-seen-to-all-your-friends/>) for products from you to your friends - and they never reveal this to you.
- When you see a like button on the web, Facebook is tracking that you're reading that page (<http://spectrum.ieee.org/podcast/telecom/internet/stalking-on-facebook-is-easier-than-you-think>). It scans the keywords on that page and associates them to you. It knows much time you spend on different sites and topics.
- They read your private messages *and* the contents of the links you send privately. (<http://www.engadget.com/2014/12/25/facebook-class-action-privacy-lawsuit/>)
- They've introduced features that turn your phone's mic on (<http://www.forbes.com/sites/kashmirhill/2014/05/22/facebook-wants-to-listen-in-on-what-youre-doing/>) -- based on their track-record ([http://www.pcworld.com/article/218528/famous\\_facebook\\_flipflops.html](http://www.pcworld.com/article/218528/famous_facebook_flipflops.html)) changing privacy settings (<http://mattmckeeon.com/facebook-privacy/>), audio surveillance is likely to start happening without your knowledge.
- They can use face recognition (<http://www.dw.de/facebook-violates-german-law-hamburg-data-protection-official-says/a-15290120>) to track your location through pictures (<http://www.makeuseof.com/tag/exif-photo-data-find-understand/>) , even those that aren't on Facebook. (Pictures taken with mobile phones have time, date and GPS data built into them.)
- They've used snitching campaigns (<http://www.digitaltrends.com/social-media/facebook-snitch-on-friends-that-arent-using-real-names/>) to trick people's friends into revealing information about them that they chose to

keep private.

- They use the vast amount of data they have on you, from your likes, things you read, things you type but don't post, to make highly accurate models (<http://www.digitaltrends.com/social-media/facebook-snitch-on-friends-that-arent-using-real-names/>) about who you are -- even if you make it a point of keeping these things secret. There are techniques, like *linear regression* which has been used in marketing for decades, that find correlating patterns between someone's behaviour and their attributes. Even if you never posted anything, they can easily work out your age, gender, sexual orientation and political views. When you post, they work out much more. Then they reveal it to banks, insurance companies, governments, and of course, advertisers.

## I HAVE NOTHING TO HIDE

A lot of people aren't worried about this, feeling they have nothing to hide. Why would they care about little old me? Why should I worry about this when I'm not doing anything wrong?

One of the more obvious problems here is with insurance companies (<http://www.insure.com/car-insurance/social-media-future.html>). The data they have on you is mined to predict your future. The now famous story of the pregnant teenager being outed by the store Target, after it mined her purchase data -- larger handbags, headache pills, tissues -- and sent her a "congratulations" message as marketing, which her unknowing father got instead. Oops!

The same is done about you, and revealed to any company without your control.

From the Terms Of Service (not the Privacy Policy -- see what they did there?):

You give us permission to use your name, profile picture, content and information in connection with commercial, sponsored or related content (such as a brand you like), served or enhanced by us.

And later:

By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.

So this includes everything they're collecting about you but not telling you. Everything you read online, everything someone ever posts about you, all your private financial transactions.

And, your data starts to get combined with your friends data to make these models more accurate. It's not just about you and your data but what gets done with all of it put together.

The issue here isn't what we have to hide, it's maintaining an important right to our freedom -- which is the right to privacy, and the right to have a say in how information about us is used. We've giving up those rights forever by using Facebook.

If you've ever admitted to something illegal in a private Facebook message, or even mentioned your support for a political cause, this can be used against you in the future, especially by another country's government. You may find yourself arrested for being at the wrong place at the wrong time, or just pulled aside at the airport one day, now facing jail time because you revealed you did something that government considers illegal 5 years ago. One New York comedian had a

SWAT team break into his house based on a joke post. Law enforcement often acts in error, and you're giving them more power and more chance of error. You're loading the gun, pointing it at your head, and handing it to every trigger-happy "enforcer" who's willing to buy your data.

There's no need to talk hypothetically about government surveillance here. One of the first Facebook investors called Greylock has board connections to a CIA investment firm called In-Q-Tel. According to their website, it "identifies cutting-edge technologies to help the Central Intelligence Agency and the broader US Intelligence Community to further their missions". And if you haven't heard - it was revealed by wikileaks that your Facebook data is delivered directly to the NSA (<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>).

And as I'll explain later, most of this information finds its way into the public anyway. No need for NSA programmes because of marketing data companies who de-anonymise all your data to sell it again and again. This is done systematically and automatically. There's an industry around this. There are marketplaces to buy and sell consumer data (<http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>), originally started around credit agencies and direct mail companies, then growing with the browser toolbar industry when Internet Explorer was big - now they're filled with more information than ever before. A recent example is RapLeaf (<https://en.wikipedia.org/wiki/TowerData>) which collected and released personally identifiable information, including Facebook and MySpace IDs. They stopped after serious controversy, but not only was the damage done, there were other companies who escaped the bad PR and kept up the same practice. It's not about how marketers target ads to you, it's that your data is bought and sold to

try.

Where might you travel in the future? Do you trust their law enforcement with this information about you? Because they're buying it.

## INTERCEPTING YOUR COMMUNICATION

The thing is that you don't need a conspiracy theory to be concerned. Mark Zuckerberg himself has been public and consistent to his investors about his intentions:

1) To be the middle-man in all personal communication.

That's why they made Messenger and bought WhatsApp, but don't forget that they've tried worse. When they made Facebook email, they took advantage of users who were syncing their Facebook contacts. They made it so everyone's @facebook.com address would be the default. Why? So that your friends would email you at your @facebook.com address instead, and they'd be able to read your emails too.

2) To make all personal communication public over time.

That's why they slowly changed the default privacy settings to public, made privacy settings harder and harder to use, and now are pretending that their privacy helper will change this.

**In reality, there a loads of privacy breaches you can't turn off, like allowing advertisers to use your endorsement to your friends, turning off how Facebook tracks what you read on the internet, or disallowing Facebook from collecting other information about you. You can't turn them off!**



## I HAVE SOMETHING TO SHARE

Even if you have nothing to hide, you have to worry about the opposite, what Facebook chooses to hide that you want to be shared. They filter you.

"I've been meaning to ask you why you're getting off" usually comes after something like, "didn't you see my post last week?"

If you've ever had that conversation, you've noticed that there's a big disconnect between your expectations when you communicate on Facebook and what really happens. Basically, Facebook filters out your posts based on whether or not people will use Facebook more if they don't see it.

It feels like Facebook is the only way to stay in touch. Through pictures and comments. It feels like everyone's on there and you're getting a good feed on their life.

**In reality, lots of your posts are never seen by anyone!** And you miss out on their stuff too. Even if your friends' stuff gets to you fine, it doesn't mean your stuff gets to them.

Private messages suck too. How many Facebook messages do you send with no reply? How many Facebook messages do you think you forget to get back to, or miss altogether? Is that how you want to treat your friends?

Facebook a really unreliable way to stay in touch.

In the last month, I simply stopped using Facebook. Something amazing happened. People phoned me, and we *really* caught up. My family was more in touch. My brother emailed me with updates. Friends popped into my place to say hi.

It was, like, social.

## POLITICAL CENSORSHIP

Facebook's blocks posts based on political content it doesn't like. They blocked posts about Ferguson and other political protests. When Zuckerberg went a bit nuts and banned the word "privacy" from meetings at Facebook, it was also blocked from any Facebook post. You just got an error message about "inappropriate content". Yeah, uh huh. Inappropriate for who?

We shouldn't be surprised though. Facebook isn't a neutral platform - we need be aware of the agendas of the people behind it. Zuckerberg's been public about his intentions. So has the first board member of Facebook - the politically conservative Peter Thiel. He wrote a book attacking multi-culturalism at Stanford, and believes in a theory called "memetic desire" which, among other things, can use people's social groups to manipulate their wants and intentions. (I'm a fan of Thiel when it comes to startups - but we often forget that everyone else out there doesn't know this stuff.)

Facebook goes so far as to let political organisations block your communication. It just takes a few people to mark the same news article as offensive, and it drops from everyone's feed. This is often abused. I can block any article from Facebook by getting a few friends to mark it as offensive. Cheap and easy censorship.

All this points to the fact that it's bad to rely on Facebook to communicate with people who are important to you. Your Facebook habit means other people have to rely on Facebook.

It's a vicious cycle.

It actually hurts your relationships with a lot of people because you think you're

in touch with them, but you're not. Those relationships fade, while your relationships with people who make "Facebook-friendly" posts take their place.

Not only does Facebook want to read all your communication, it wants to control it too.

## RATTING ON YOUR FRIENDS

Even if you're sort of okay with this for you, by using Facebook, you're forcing your friends and family to accept the same. Even the ones who aren't on Facebook or go as far as to use fake names.

If you've ever used Facebook contact sync, or used Facebook on your mobile phone, Facebook took your complete contact list. Real names, phone numbers, addresses, emails, everything. They then use that to create "shadow profiles" of the people you know who aren't on Facebook ([spectrum.ieee.org/podcast/computing/networks/facebook-knows-your-friendseven-if-theyre-not-on-facebook/](http://spectrum.ieee.org/podcast/computing/networks/facebook-knows-your-friendseven-if-theyre-not-on-facebook/)). Non Facebook users often see this in action, in the form of emails to them from Facebook, containing their personal information. Facebook users can see this when they upload a picture of a non-Facebook user, and they're automatically tagged. My friend's not on Facebook, but since me and a few friends used Facebook on our phones, Facebook has his name and contact information, plus knows who his friends are because it sees him in their address book and calling records. A couple of pictures uploaded with his face, and presto - they can identify him in pictures -- adding location data from the pictures to his shadow profile. Lots of Facebook's other techniques work on shadow profiles too. They can very accurately infer a lot about him from who his friends are.

So basically, we've all inadvertantly been ratting on our friends who wanted to remain private. Facebook tricked us.

But Facebook's tricks go further.

## "PRIVACY" DOESN'T APPLY TO WHAT FACEBOOK DIGS UP

Like shadow profiles of people, Facebook can "infer a like" (<http://www.forbes.com/sites/anthonykosner/2013/08/31/new-facebook-policies-sell-your-face-and-whatever-it-infers/>) based on other information it has about you, like what you read all over the internet or what you do in apps where you log in with Facebook. Call it a "shadow like." This allows them to sell you to more advertisers.

It's already well-documented that Facebook collects this information. The "shadow like" technique is simply the standard use of statistical techniques in database marketing ([https://en.wikipedia.org/wiki/Database\\_marketing](https://en.wikipedia.org/wiki/Database_marketing)); if you read a lot about a topic, you probably like it. These are techniques used in marketing since the 80s, and you can hire university statistics students to do them, though of course, Facebook hires the best in the field. In Europe, Facebook is legally obliged to share exactly how it does this - but they refuse. So there's another class action lawsuit against them. (<http://europe-v-facebook.org>)

Through its labyrinth of re-definitions of words like "information", "content" and "data", you're allowing Facebook to collect all kinds of information about you and expose that to advertisers. With your permission only they say, but the definition of "permission" includes using apps and who knows what else.

And you thought those Farmville requests were annoying. Every time you saw one, that friend was revealing your information to "third parties."

So effectively, all that stuff you marked as "friends only" doesn't matter so much.

By being on Facebook, there's way more information about you that's collected, combined, shared, and used.

They say they "anonymise" this, but in reality, it's a simple step to de-anonymise it. A lot of the anonymous data, like what and when you posted, pictures of you, your location at a given time, is enough for a huge number of companies to tie that anonymous data back to you -- and sell it on.

On top of this, they allow all the Facebook apps full access to your information - with your name and everything. And even if you never use any apps on Facebook, your friends do. When they use apps, your friends share all your information for you. There's a whole industry behind this.

Some things DO have off buttons, but keep in mind they are temporary, and will be switched back on without letting you know. When Facebook started (and probably when you joined) it was clearly a safe place to share with **your friends only**. That was their big promise. Over time, they switched the default privacy setting to public so that if you still wanted to keep Facebook for friends only, you had to manually find over 100 settings on multiple hidden settings pages. Then, they started dropping those settings and forced information to be public anyway.

Why are you *still* punching yourself? :)

## SELLING YOUR ENDORSEMENT WITHOUT YOUR CONSENT

You might have noticed Facebook ads with your friends' endorsement under it. Basically, Facebook gives advertisers the right to use you as an endorser, but you have no control over it. It's not limited to when you've actually clicked a like button. There have been known cases of vegetarians endorsing McDonalds, a

long- and happily-married woman endorsing dating sites, and even a young boy endorsing a sex club to his own mother!

Those cases were so embarrassing that the person found out. People called them up. But in most cases, these are endorsements that don't get discovered -- people assume them to be true. That's even scarier because Facebook is used heavily for political advertising, and product endorsements. People know I raised money for kids with cancer before, so they might not be surprised if they see an ad where I'm endorsing a Christian outreach programme poor kids in Africa. But I categorically only support programmes that don't have religious allegiances, since they're known to bias their support to people who convert. Worse, a lot of people might assume things about my religious beliefs based on these false endorsements. Don't even get me started on all the hypey startup stuff I don't condone!

Using Facebook means this happens all the time. Advertisers can buy your endorsement and all your information. You never get to know about it, and you can't turn it off.

## THE LATEST PRIVACY CHANGE

Finally, I want to explain how this latest privacy change makes things way worse, and way more out of your control if you stay on Facebook.

Facebook is demanding to track what you buy, and your financial information like bank account and credit card numbers. It's already started sharing data with Mastercard (<http://www.theage.com.au/it-pro/business-it/mastercard-to-access-facebook-user-data-20141006-10qrqy.html>). They'll use the fact that you stayed on Facebook as "permission" to make deals with all kinds of banks and financial institutions to get your data from them. They'll call it anonymous, but like they

trick your friends to reveal your data to the third-parties with apps, they'll create loopholes here too.

Facebook is also insisting to track your location via your phone's GPS, ***everywhere and all the time***. It'll know exactly who you spend your time with. They'll know your habits, they'll know when you call in sick at work, but are really out bowling. "Sal likes 2pm Bowling at Secret Lanes." They'll know if you join an addict support group, or go to a psychiatrist, or a psychic, or a mistress. They'll know how many times you've been to the doctor or hospital, and be able to share that with prospective insurers or employers. They'll know when you're secretly job hunting, and will sell your endorsement for job sites to your friends and colleagues -- you'll be revealed.

They'll know everything that can be revealed by your location, and they'll use it however they want to make a buck.

And -- it'll all be done ***retrospectively***. If you stay on Facebook past January 30th, there's nothing stopping all of your past location and financial data to get used. They'll get your past location data from when your friends checked-in with you, and the GPS data stored in photos of you. They'll pull your old financial records - that embarrassing medicine you bought with your credit card 5 years ago will be added to your profile to be used as Facebook chooses. It will be sold again and again, and likely used against you. It will be shared with governments and be freely available from loads of "third-party" companies who do nothing but sell personal data, and irreversibly eliminate your privacy.

Why irreversible, and why now?

Location and financial data are not just really sensitive, they allow the "third-parties" de-anonymise information about you. (<http://www.pcworld.idg.com.au>

/article/565150/how-three-small-credit-card-transactions-could-reveal-your-identity/) This massively empowers these third-parties to collect all available information about you, including calculated information that you never revealed. This is a situation where even Facebook itself will have trouble maintaining the privacy of its data -- not that they care.

This is unprecedented, and just like you'd never have guessed that Facebook would sell your endorsements when you signed up in 2009, it's too hard to predict what Facebook and those third-party data sellers will do with this new power.

This isn't a prediction, it's a direct consequence of their current business model. **Facebook sells you out, because that's exactly how they make money.** And they're under heavy pressure from their investors to make more.

There's nothing you can do about this. Facebook gives you two options: accept all of this, or get off the Facebook bus.

To be honest, this bus is getting loud, annoying and bit smelly, isn't it? And the ticket is way too expensive in the first place.

## HOW TO GET OUT OF THIS MESS

According to the FTC settlement from a few years ago, after Facebook was sued by the US government for its privacy practices, Facebook is "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;"

There are different interpretations of this. Some say you need to delete each post separately, others say delete your account, and some say they'll still keep your data anyway -- that all you can do is stop giving them more data.



I'm going to do all of them. There are a few helpful browser add-ons that will delete your posts individually (<http://activityremover.com/>), and some great instructions on actually deleting your account (<http://lifehacker.com/5813506/how-to-delete-your-facebook-account>) while Facebook tries to trick you into deactivating it instead.

Then there are all the apps you've used. This is one of Facebook's best loopholes because they say they can't control what the apps do with your data once you give it to them. So, I've saved the settings page that shows what apps I've used onto my hard drive, and removed access to each of them manually. Each of those apps have their own privacy policy -- most of them are a lost cause, claiming unlimited rights to my data, so I'm just shutting them down and moving on.

To stop Facebook from tracking what I read on the web, (they do this even if you don't have a Facebook account) I've installed Ghostery (<http://ghostery.org>). (And while you're at it, the EFF made this great plugin that automatically chooses the most secure web connection (<https://www.eff.org/https-everywhere>), making it more difficult for governments and ISPs to snoop your web activity.)

FrostBox (<http://www.frostbox.com>)'s free trial seems to be working for quickly saving my Facebook photos and videos. For other information, I used Facebook's archive found under general settings. (It includes pictures, but not full size.)

I also downloaded my friends page - just by scrolling to the bottom, and hitting File -> Save. Worst case, I can still see your publicly listed contact info if I don't have it somewhere else. (Honestly, so far I haven't needed the file yet.)

If you have any other ideas or advice, please get in touch. This is what I see as a responsible step to prevent myself, my family and my friends from having their freedom taken from them, and their personal relationships made to suffer.

Lastly, the world is full of people who say “it’ll never happen”, and when it does, they switch to “there’s nothing we can do.” There is. (<https://medium.com/@SaintSal/you-are-our-first-defence-b86ae9a1fff6>) We have a say in the world we want to live in. We can help everyone understand, and make their own informed choices.

Please share this with people who are important to you. (And catch yourself in the habit - were you about to post this to Facebook? Email it, or better yet phone!)

## SOURCES

A note on the quality of these sources: I tried to find references from major news outlets, with a range of political biases. These articles are less technically aware, but we can expect they're more rigorous than blogs at checking their sources. For the more technical stuff, sources like The Register are known to be more credible, and Techcrunch is notoriously unreliable at fact-checking. I've included some of their articles though, because they're good at explaining things.

Facebook likes reveal sensitive personal information

eff.org (<https://www.eff.org/deeplinks/2013/03/facebook-likes-reveal-sensitive-personal-information>)

Private traits and attributes are predictable from digital records of human behavior

pnas.org (<http://www.pnas.org/content/110/15/5802.full>)

table of top likes (<http://www.pnas.org/content/suppl/2013/03/07/1218772110.DCSupplemental/st01.pdf>)

New Facebook Policies Sell Your Face And Whatever It Infers

forbes.com (<http://www.forbes.com/sites/anthonykosner/2013/08/31/new->

facebook-policies-sell-your-face-and-whatever-it-infers/)

You are what you Facebook Like

washingtonpost.com (<http://www.washingtonpost.com/news/the-intersect/wp/2014/10/29/you-are-what-you-facebook-like/>)

Criticism of Facebook - Wikipedia, the free encyclopedia

en.wikipedia.org ([http://en.wikipedia.org/wiki/Criticism\\_of\\_Facebook](http://en.wikipedia.org/wiki/Criticism_of_Facebook))

Facebook

stallman.org (<https://stallman.org/facebook.html>)

Forcing users onto Messenger

huffingtonpost.com ([http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face\\_b\\_4365645.html?fb\\_action\\_ids=800240053354677&fb\\_action\\_types=og.likes&fb\\_source=other\\_multiline&action\\_object\\_map=\[224913967679581\]&action\\_type\\_map=\[%22og.likes%22\]&action\\_ref\\_map=\[\]](http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html?fb_action_ids=800240053354677&fb_action_types=og.likes&fb_source=other_multiline&action_object_map=[224913967679581]&action_type_map=[%22og.likes%22]&action_ref_map=[]))

Permissions

telegraph.co.uk (<http://www.telegraph.co.uk/technology/facebook/11217273/Facebooks-Mark-Zuckerberg-Why-I-wear-the-same-T-shirt-every-day.html>)

WhatsApp

hackread (<http://hackread.com/whatsapp-facebook-privacy-data-share/>)

Europe vs Facebook

irishtimes.com (<http://www.irishtimes.com/business/technology/more-than-20-000-join-privacy-action-against-facebook-1.1889192>)

<http://www.slate.com/blogs/future> (<http://www.slate.com/blogs/future>) **tense**  
**/2014/05**  
**/01/a-developer-tools-users-can-login-with-facebook-but-stay-anonymous.html**

<http://europe-v-facebook.org./EN/Objectives/objectives.html> (<http://europe-v-facebook.org./EN/Objectives/objectives.html>)

Facebook info sharing created Zoosk.com dating profile for married woman  
cbc.ca (<http://www.cbc.ca/1.2844953>)

@facebook.com e-mail plague chokes phone address books arstechnica.com  
(<http://arstechnica.com/business/2012/07/facebook-com-e-mail-plague-chokes-phone-address-books/>)

Facebook Knows Your Friends—Even if They're Not on Facebook - IEEE Spectrum  
spectrum.ieee.org (<http://spectrum.ieee.org/podcast/computing/networks/facebook-knows-your-friendseven-if-theyre-not-on-facebook/>)

Facebook Now Wants To 'Spy' On Android Phone Users!  
efytimes.com (<http://www.efytimes.com/e1/fullnews.asp?edid=128859>)

Facebook adds naggy “ask” button to profile pages  
arstechnica.com (<http://arstechnica.com/business/2014/05/facebook-introduces-naggy-ask-function-into-profile-pages/>)

Facebook users unwittingly revealing intimate secrets, study finds  
theguardian.com (<http://www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets>)

Facebook's Generation Y nightmare  
theguardian.com (<http://www.theguardian.com/technology/2012/sep/24/facebook-generation-y>)

Facebook Knows Your Friends—Even if They're Not on Facebook - IEEE Spectrum  
spectrum.ieee.org (<http://spectrum.ieee.org/podcast/computing/networks/facebook-knows-your-friendseven-if-theyre-not-on-facebook/>)

Facebook's New Privacy Rules Clear the Way for Payments Push and Location-Based Ads

recode.net (<http://recode.net/2014/11/13/facebooks-new-privacy-rules-clear-the-way-for-a-payments-push-and-location-based-ads/>)

Dutch Regulator Investigates Facebook's Privacy Policy

bits.blogs.nytimes.com (<http://bits.blogs.nytimes.com/2014/12/16/dutch-regulator-investigates-facebooks-privacy-policy/>)

Facebook prunes its privacy policy, lays groundwork for location-based ads - GeekWire

geekwire.com (<http://www.geekwire.com/2014/facebook-gives-privacy-policy-haircut-adds-provisions-payment-location-based-ads/>)

Stalking on Facebook Is Easier Than You Think - IEEE Spectrum

spectrum.ieee.org (<http://spectrum.ieee.org/podcast/telecom/internet/stalking-on-facebook-is-easier-than-you-think>)

Millions Will Flow to Privacy Groups Supporting Weak Facebook Settlement | WIRED

wired.com (<http://www.wired.com/2012/07/groups-get-facebook-millions/all/>)

Facebook Is Recycling Your Likes To Promote Stories You've Never Seen To All Your Friends

forbes.com (<http://www.forbes.com/sites/anthonykosner/2013/01/21/facebook-is-recycling-your-likes-to-promote-stories-youve-never-seen-to-all-your-friends/>)

Is Facebook damaging your reputation with sneaky political posts? | ZDNet

zdnet.com (<http://www.zdnet.com/article/is-facebook-damaging-your-reputation-with-sneaky-political-posts/>)

Even Google won't be around for ever, let alone Facebook  
theguardian.com (<http://www.theguardian.com/technology/2013/mar/03/google-facebook-nothing-lasts-for-ever>)

Facebook reforms user settings  
dailyemerald.com (<http://dailyemerald.com/2010/05/27/facebook-reforms-user-settings/>)

Facebook Privacy: A Bewildering Tangle of Options - Graphic - NYTimes.com  
nytimes.com ([http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html?\\_r=0&ref=personaltech](http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html?_r=0&ref=personaltech))

Corrupt Personalization  
blogs.law.harvard.edu (<http://blogs.law.harvard.edu/niftyc/archives/1003>)

Facebook is not your friend  
theguardian.com (<http://www.theguardian.com/commentisfree/andrewbrown/2010/may/14/facebook-not-your-friend>)

Facebook violates German law, Hamburg data protection official says | Sci-Tech | DW.DE | 02.08.2011  
dw.de (<http://www.dw.de/facebook-violates-german-law-hamburg-data-protection-official-says/a-15290120>)

The World from Berlin: 'Every User Can Decide Alone What Facebook Knows' - SPIEGEL ONLINE  
spiegel.de (<http://www.spiegel.de/international/germany/critique-of-german-credit-agency-plan-to-mine-facebook-for-data-a-837713.html>)

Q&A: Facebook privacy changes  
bbc.co.uk (<http://www.bbc.co.uk/news/10165573>)

Famous Facebook Flip-Flops

pcworld.com ([http://www.pcworld.com/article/218528/famous\\_facebook\\_flipflops.html](http://www.pcworld.com/article/218528/famous_facebook_flipflops.html))

No Death, No Taxes - The New Yorker

newyorker.com (<http://www.newyorker.com/magazine/2011/11/28/no-death-no-taxes>)

Facebook censors political satire after complaint from JobCentre Plus

tompride.wordpress.com (<http://tompride.wordpress.com/2013/04/25/facebook-censors-political-satire-after-complaint-from-jobcentre-plus/>)

TED: The curly fry conundrum: Why social media “likes” say more than you might think

tedtranscripts.blogspot.com (<http://tedtranscripts.blogspot.com/2014/10/the-curly-fry-conundrum-why-social.html>)

With friends like these ... Tom Hodgkinson on the politics of the people behind Facebook

theguardian.com (<http://www.theguardian.com/technology/2008/jan/14/facebook>)

Facebook Must Face Lawsuit Over Scanning of Users' Messages, Judge Says

recode.net (<http://recode.net/2014/12/24/facebook-must-face-lawsuit-over-scanning-of-users-messages-judge-says/>)

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

forbes.com (<http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>)

War on General Purpose Computers is the difference between utopia and

dystopia

boingboing.net (<http://boingboing.net/2014/12/26/war-on-general-purpose-compute.html>)

Don't Worry About Selling Your Privacy To Facebook. I Already Sold It For You | Just Well Mixed

jasonlefkowitz.net (<http://jasonlefkowitz.net/2011/10/dont-worry-about-selling-your-privacy-to-facebook-i-already-sold-it-for-you/>)

Facebook's Hidden "Like" Isn't Just Good For Mobile Developers, It's Good For Facebook

techcrunch.com (<http://techcrunch.com/2012/06/26/facebooks-hidden-like-isnt-just-good-for-mobile-developers-its-good-for-facebook/>)

Mastercard to access Facebook data

theage.com.au (<http://www.theage.com.au/it-pro/business-it/mastercard-to-access-facebook-user-data-20141006-10qrqy.html>)

Three transactions can reveal your identity

pcworld.idg.com.au (<http://www.pcworld.idg.com.au/article/565150/how-three-small-credit-card-transactions-could-reveal-your-identity/>)

Look who's lurking around your Facebook page: Your insurance company!

insure.com (<http://www.insure.com/car-insurance/social-media-future.html>)

NSA Prism program taps in to user data of Apple, Google and others

theguardian.com (<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>)

Everything We Know About What Data Brokers Know About You

propublica.org (<http://www.propublica.org/article/everything-we-know-about->



what-data-brokers-know-about-you)

## MAKE BETTER STARTUP DECISIONS

I write about making better startup decisions from first-hand experience, and teaching in accelerators across Europe. I write all over the web - so subscribe

(<http://saintsal.us4.list-manage1.com>

[/subscribe?u=cd94a6d414d0d34e19cddf5bd&id=d740a24578](http://saintsal.us4.list-manage1.com/subscribe?u=cd94a6d414d0d34e19cddf5bd&id=d740a24578)) for email updates whenever I post.

✉ (<http://saintsal.us4.list-manage1.com>

[/subscribe?u=cd94a6d414d0d34e19cddf5bd&id=d740a24578](http://saintsal.us4.list-manage1.com/subscribe?u=cd94a6d414d0d34e19cddf5bd&id=d740a24578))

📡 (<http://saintsal.com/rss/>)

## SHARE

Please share this post if you think it's useful.

🐦 ([http://twitter.com/share?text=Get your loved ones off Facebook.&url=http://saintsal.com/facebook/](http://twitter.com/share?text=Get%20your%20loved%20ones%20off%20Facebook.&url=http://saintsal.com/facebook/))

**f** (<https://www.facebook.com/sharer/sharer.php?u=http://saintsal.com/facebook/>)

**g+** (<https://plus.google.com/share?url=http://saintsal.com/facebook/>)





## SALIM VIRANI

Founded 5 startups & seen 3 bubbles. I started Leancamp, where founders share what actually works for them, and Founder-Centric, known for our practical, attitude-shifting way of teaching startups.

Get in touch:  (<http://twitter.com/saintsal>)  (<http://saintsal.com/contact>)

All content copyright SaintSal (/) © 2013 • All rights reserved.