Privacy Theater: Why Social Networks Only Pretend To Protect You

by Guest Author on December 27, 2009

Editor's note: The following guest post was written by Rohit Khare, the co-founder of Angstro. Building his latest project, social address book Knx.to, gives him a deep familiarity with the privacy policies of all the major social networks.

I'd be wishing everyone a happier New Year if it were easier to mail out greeting cards to friends on Facebook and colleagues on LinkedIn. I'd like to use knx.to, our free, real-time social address book, but their 'privacy' policies prevent us from downloading contact information, even for my own friends.

At least those Terms of Service (ToS) that force us to copy addresses and phone numbers one-by-one also prevent scoundrels from stealing our identity; reselling our friends to marketers; and linking our life online to the real world. Right?

Wrong. When RockYou can stash 32 million passwords in the clear; when RapLeaf can index 600 million email accounts; and when Intelius can go public by buying 100 million profile pages; then our social networks have traded away our privacy for mere "privacy theater."

With apologies to Bruce Schneier's brilliant coinage, "security theater" (e.g. the magical thinking behind forcing passengers to sit down and shut up for the last hour of international flights), social networks have been dogged by one disaster after another in 2009 because they pursue policies that provide the "feeling of improved privacy while doing little or nothing to actually improve privacy."

As long as the same information that social networks piously prohibit their own customers from using is being bought and sold on the open market by giant marketing companies, social networks are only pretending protect your privacy.

Industrial-Scale Identity Theft

Last week's headlines brought news that RockYou had accumulated 32,603,388 identities over the past few years — and negligently stored them in plaintext in an incompetently protected database.

RockYou's official bluster about "illegal intrusion" should fool no one: blaming Imperva, the firm who exposed the flaw, or accusing the hacker(s) of being the identity thieves is misdirection: it was actually RockYou who stole those credentials, and RockYou should be held to account.

I realize that I'm using the incendiary terms "identity theft" and "stole," even though I would agree that users voluntarily consented to type their passwords into RockYou's forms. I assume that both users and RockYou's developers actually only intended to share some particular bits of information: a contact list, a user photo, a friend's gender; but the bottom line is that instead of sharing that specific data, RockYou retained enough secrets to impersonate those users at will.

* Don’t blame the victims. Bemoaning the absence of open standards for users to share their own data; or complaining about the weaknesses of users’ password choices is merely changing the subject.
* Don’t blame “security” technology. More encryption, better encryption, or stronger firewalls would not help, since the default RockYou username in this case was a user’s primary email address. For anyone who chose to use a popular Webmail service, that granted access to every other online service they’ve ever used — because of those ubiquitous “Forgot your password?” buttons to email it back to you (just ask Twitter how much fun that is).
* Don’t blame RockYou’s partners, who hosted their widgets. They just wanted to give their users some fancy new slideshows and scoreboards and other features to put on their pages; that shouldn’t have required an all-out war for viral growth that demanded users to log in and advertise their new widgets to all of their friends.

The fault, dear Reader, is not in our stars; it lies with sites that pretend to waive all care and duty by idly warning their users not to share their account passwords with anyone else.

In the absence of vigorous enforcement of those ToS agreements, any RockYou developer who passed up the opportunity to, say, phish MySpace passwords was putting their own employer at a disadvantage to any other startup that was willing to race them to the bottom.

APIs: Automating Privacy Intrusions?

RockYou minimized the scope of this breach by maintaining that it only affected their “legacy platform” for widgets rather than its larger “partner applications platforms” that use “industry standard security protocols.” After all, the advent of social networks’ partner APIs was supposed to make impersonation and scraping obsolete.

Those APIs came with their own new ToS agreements that added new, overlapping, and sometimes-contradictory restrictions as they worked through all of the implications of letting third parties in on the fun. The ACLU released a fun quiz that makes quite clear how much information is at stake, from your hometown to your friends’ sexual orientation.

For example, if you upload a photo of me that I find embarrassing, I could prevent you from tagging me in it, but I can’t forbid you from keeping your own photo online (or keeping it private, bugs aside). I can’t even forbid another friend of ours from caching a copy in his or her browser.

However, the Facebook API ToS can (and does) prevent a third-party application from caching a link to the photo for more than a day (a week on Orkut). Unfortunately, direct links to the photo server didn’t double-check the privacy policy, so a third-party app would be at risk of leaking images users thought were private, unless the developer remembered to make a separate API call every time to re-verify every photo on a page.

He (or She) Who Must Not Be Named

In an ideal world, a third party developer shouldn’t have to store any personally-identifiable information (PII). In many jurisdictions, PII is akin to toxic waste, because of the regulatory burdens and civil, even criminal, liability for acquiring and disposing of it.

Here again, Facebook is the pacesetter: it’s possible to display “She liked 7 photos uploaded by Mr. Smith two weeks ago” using little more than a numeric user id. The developer writes a sentence in Facebook Markup Language (FBML), and Facebook’s servers will dynamically substitute the name,

gender, item count, and ensure grammatical agreement of pronouns, singular/plural choices, and time intervals.

OpenSocial gadgets have to copy PII into the browser to format a sentence like that. LinkedIn's partners even have to copy PII to their own servers, since their Open API is currently incompatible with AJAX authentication.

Even though copying PII is the root of all privacy risks, there are three reasons it can be necessary: latency, history, and agility. Without caches, slow API calls can make an app's performance suffer. Without archives, analyzing only the most recent events can mislead an app's trend detection or recommendation services. Without "offline" access, waiting for a user to log in again delays an app's reaction to events in real-time.

There aren't many technical countermeasures once data has been copied. LinkedIn spent more than a year tinkering with their public API, but the only substantial difference is that it now encrypts every member id with the identity of the developer and application to trace the source of a breach. I applaud them as an industry pioneer — though they're so dependent on search-engine optimization that they still include the public numeric ids in the profile page URLs anyway.

Exporting PII with legal strings attached is the best policy we can hope for. While Amazon's ToS requires its associates to display accurate, up-to-date prices, Twitter has only recently realized the implications of searching deleted tweets and doesn't yet oblige its API partners to update their copies when tweets are deleted or protected.

Buying Back Your Own Data? Priceless.

If PII is so hard to protect, then the only way for social networks to protect their users' privacy must be to prohibit partners from accessing contact information in the first place. I might not be able to export my holiday card mailing list from my favorite social network— a roach motel for our data — but giant marketing corporations can buy and sell our private information with impunity.

I could go to Rapleaf right now to buy an analysis of any list of email addresses to learn its makeup by gender, income, residence, and all manner of other demographic data. Who's to say how short that list could be—it's a slippery slope from aggregate info to personal info. Or I could shop at one of Intelius' many fronts and affiliates who are selling PII explicitly (TRUSTe-certified!). Or I could barter some of the stray business cards on my desk on Jigsaw to fill in the rest of the puzzle. All of these businesses depend on PII data harvested from social networks.

How is that possible? None of the social networks that we've integrated with has an API for reading email addresses — but all of them have no problem asking you to "Invite your friends!" After all, most social networks remain hypocritical enough to phish passwords to other social networks themselves as soon as they ask you to "Invite your friends" for their own viral growth!

Putting aside the hypocrisy of phishing passwords to scrape those friends' email addresses in the first place, the subtler flaw is that social networks are more than happy to search their member database for those addresses to share a list of suggested friends. That's how a Rapleaf could take a mailing list, pretend that those are all friends of theirs, and slowly accumulate a "reverse phonebook" that maps emails to social network profiles.

Or you could just crawl their websites. Social networks depend on search engines for traffic, so they

almost universally have public pages for every member with well-known URLs and directory listings by name for crawlers to index. A mini-boomlet in funding "people search" startups underwrote this massive exercise, but they sold their archives to less-than-savory marketers.

Now, merely indexing public web pages can't be evil—but reconciling online identities and 3rd-party advertising cookies with real-world credit reports, government records, and other databases can be. Adding in all that information doesn't increase Mr. Smith's anonymity; Jeff Jonas has made a small fortune proving that semantic reconciliation dramatically collapses uncertainty. Just think about combining Spock's 100M profiles with Intelius' 20B other data points; or Wink's 200M profiles with Reunion MyLife's 34M members and 700M records…

Whose Data Is It, Anyway?

The philosophical question at hand is what rights do I have in my friends' information. When I accept a business card from someone I've just met, I don't believe I have the right to re-sell it on Jigsaw in good conscience (they'd disagree 18M times). If it's a colleague's card, on the other hand, I might take the initiative to forward a new lead, or even buy a gift subscription to a magazine. Does that constitute a violation of their privacy, or spam?

Social networks haven't let their users make their own decisions on this issue. Through selective enforcement of their policies, some startups get locked out while big partners get exemptions. Power.com ended up in (and out of) court. Plaxo found out the hard way that they couldn't assist their paying customers to OCR Facebook email addresses; or to synchronize with LinkedIn. It says a lot about LinkedIn's draconian ToS that even with paying customers demanding it, Comcast hasn't signed up for their API. Even if users manually download their own LinkedIn address books, it won't even include links back to folks' public profile pages.

Don't Accept Incompetence

I also claim that social networks are engaging in Privacy Theater because there's no shortage of examples of organizations on the Web that process vast quantities of PII while providing real privacy protection. Do you think that the "bad guys" haven't gone after Webmail services to phish passwords and harvest contact information? Aren't e-commerce sites sharing product information and reviews out to legions of affiliates without leaking your purchase history? How long do you think RockYou would have gotten away with it if they were asking for your online banking username instead of your email address?

Social network sites have not (yet) demonstrated the high degree of proactive surveillance and enforcement characteristic of other organizations that deal with PII on the Internet. Users see worms on MySpace and viruses on Facebook, but not on Hotmail — because they defend against cross-site-scripting attacks. Users find malware distributed on Slide, but not on Wikipedia — because they filter content aggressively. Users are blocked by DDoS attacks and DNS attacks on Twitter — but Amazon stays up because they can react in real-time (mostly). How much more quickly do Cease & Desist letters for putting up a fake PayPal logo go out than for impersonating a Facebook Page?

From personal conversations, I'm beginning to wonder if the recent rise of Hadoop is part of the problem, surprisingly. Trying to detect patterns of abusive crawling and suspicious bursts of activity from partner apps by analyzing yesterday's log files alerts you too late to react. The culture of many social networking websites seems to emphasize page load times (especially after the great Friendster meltdown), which isn't quite the same as the enterprise IT, networking, and transactional database backgrounds of other leading Web architects. And unlike the formal (and informal) networks of

security officials at online financial institutions to track distributed threats, I fear we have little evidence of coordinated responses to privacy threats that correlate identities across social networks.

I have first-hand experience that it takes more time (and more money) to ship applications that comply with social networks' privacy policies. If we weren't living with Privacy Theater, that might not have been a wasted investment. Inevitably, Gresham's Law kicked in, and the good guys are being driven out by the bad guys (spammy apps, scammy apps, sneaky apps, conniving apps).
Privacy Theater: The Show Must Go On…

Naturally, I prefer to think of myself as one of the 'good guys.' I prefer to believe that privacy protection is a competitive advantage that users (citizens!) really value. Until this outrageous RockYou breach, I didn't fully realize how irrelevant that is.

I'd argue that the hapless state of ToS enforcement by the major social network platforms only provides the feeling of improved privacy while doing little or nothing to actually improve privacy: that's privacy theater.

Unfortunately, that analogy is still unfair: TSA may screen children at the airport, but at least their security theater doesn't obscure the fact we haven't had a catastrophic security failure in the US air transportation system (yet). Our major social networks' privacy theater is distracting us from ongoing, large-scale identity theft and misuse of private and personally-identifiable information.

If the industry expects self-regulation to forestall government regulation, well, here's what I think it would take: An immediate ban on all of RockYou's applications by all of their partners, pending a public audit of all of their apps. That's taking a page from the audit provisions of LinkedIn's ToS and adding sunlight by publishing the results.

Sounds harsh? I thought the market was supposed to provide swifter, surer justice than some pesky regulator with its clunky old notions of due process and presumptions of innocence. API agreements are a private matter between ruthless corporations. Heck, if they really wanted to put the rest of the ecosystem on notice, they ought to audit every application funded by Sequoia, Partech, DCM, and Softbank, all lead investors in RockYou.

It's not like lawsuits are being filed, as Marissa Mayer announced by going after work-from-home scam artists in an interview with Mike Arrington at LeWeb. It's not like this is Scamville 2.0, since this isn't stealing users' cash, only their dignity. It's not like there's a legal spotlight on the issue, since there's only $9M set aside for a hazy new privacy foundation in the latest Facebook class-action settlement. It's not like it's a political issue in the headlines, since a Facebook Chief Privacy Officer is running for Attorney General, the top law-enforcement office in California. It's not like it's as complicated as "don't be evil," since I can give you one simple tip to eliminate privacy theater: enforce your ToS and obey others' ToS — or else stop setting unrealistic expectations and just let users have their data back!

(Photo credit: Flickr/FaceMePLS).
get widgetminimize
CrunchBase Information
Rohit Khare
Rohit Khare image
Companies: Angstro

Rohit is an award-winning researcher in the fields of Internet protocols and decentralized systems. He founded KnowNow in 2000 and previously worked on Internet standards development at MCI's Internet Architecture Group and the World Wide Web… Learn More
RockYou
RockYou image
Website: rockyou.com
Location: Redwood City, California, United States
Founded: November, 2005
Funding: $119M

Netpickle maker of RockYou (originally named RockMySpace) creates and distributes self-expression widgets. The widgets can be used to enhance the look and feel of blogs, personal websites and personal pages on social networks such as Facebook,… Learn More
Information provided by CrunchBase

Next Post
Previous Post

* Actively Discussed Posts

* TSA To Save Print Media? No Electronics On International Flights? What A Joke.
  216 comments
* NSFW: The Physical Impossibility of The Future in the Mind of Someone Trapped In Chicago
  181 comments
* 370 Passwords You Shouldn't (And Can't) Use On Twitter
  124 comments
* Should You See Avatar? About 75 Percent Of People Who Tweet About It Think You Should
  99 comments
* Apple Expanding iWork In The Cloud?
  39 comments

Responses

* bookmarking » Blog Archive » Privacy Theater: Why Social Networks Only Pretend To Protect You
  December 27th, 2009 at 11:10 pm
* Privacy Theater: Why Social Networks Only Pretend To Protect You | searching phone
  December 28th, 2009 at 4:17 am

Comments rss icon

*
Andrew (@styleguidance) - December 27th, 2009 at 11:09 pm PST

if companies cared about privacy, the default privacy setting would be set to 100% private. Instead of the other way around
reply
o
magnum - December 28th, 2009 at 7:18 am PST

Apart from what Mark Zuckerberg said, I guess individual facebook users should practice security measures on their own in order to avoid attacks and other privacy issues.

Hackers will always be around and it would be an enormous undertaking for facebook to manage 350 million subscribers 24/7: http://bit.ly/a...acebook-hacking

Alas, Total Privacy on the internet is a myth and that's why we should understand that 'what you kept inside your borders in real life, should be kept from the cyber world as well. No special treatment
reply
*
Clint Pee
Clint Pee - December 27th, 2009 at 11:14 pm PST

Most people want their info to be public It helps them get known in the internet world.

The Padrino
http://www.thepadrino.com
reply
o
JontheBod - December 27th, 2009 at 11:37 pm PST

Ummm – 'most people' is a baseless and inconsequential notion you're proffering. As long as 'some people' don't feel as you assume, they need appropriate safeguards to ensure their wishes are honored.
reply
o
dave hanna - December 27th, 2009 at 11:58 pm PST

Most people want to make their info public to their friends, not to everyone. Bloggers like to be known so they can sell ad space. FB posters by in large are not bloggers selling their space
reply
o
Leif Andersen (@LeifAndersen) - December 28th, 2009 at 7:27 am PST

While I have my stuff public, it seams like most people would rather have their stuff private, as they are worried about 'creeps'.
reply
*
anonymouse - December 27th, 2009 at 11:23 pm PST

Damn Good Article.

Facebook is just as criminal and has the fleece over everyone's eye. Privacy Policies are a way for Facebook to keep the data to themselves making them even more powerful.

reply

- Pete Austin - December 28th, 2009 at 3:27 am PST

  Yes: article is concise and well-researched, with lots of appropriate references. Essential reading for everyone who belongs to a social network, or works for one. But disagree they are criminal.

  reply

*

Jay Cuthrell (@qthrul) - December 27th, 2009 at 11:44 pm PST

Great summary.

This is timely considering the discussion over at GigaOm on the happy-shiny-possible-new-layout for a home view on Facebook vs. a treatment of where granular Facebook permissions may alter in subsequent site revisions.

reply

*

Saami Matloob
Saami Matloob - December 27th, 2009 at 11:47 pm PST

truly an eye opener on privacy theater.

Like it

reply

*

Freakyincubator (@freakyidea) - December 28th, 2009 at 12:15 am PST

Nice read. Its really tough for the user to read beyond the line. There should be an agency which should authenticate the privacy policy followed by the website.

reply

*

Nibras Bawa (@nibrasbawa) - December 28th, 2009 at 12:16 am PST

Well said. Talking privacy on social networks (or internet for that matter) is like talking virginity with a prostitute in a brothel. Its difficult for them to co-exist :)

reply

*

Rotten Owl Sheep (@rottenowlsheep) - December 28th, 2009 at 1:22 am PST

Really good article and insight. Time to reconfigure all my accounts.

reply

*

k - December 28th, 2009 at 2:04 am PST

Zuckerburg wrote the book on how to f people over.

Related to this, the question that pop ups in my mind is those who support F Connect aren't they supporting this kind of behavior?

It's like buying blood diamonds. It's difficult to know if that's what you're buying (not the case here) but when you do buy them you know you're funding slavery, rape, war.

This goes beyond talking about privacy but the principles are they same.

You shouldn't F people over, nor should you support or make use of a system that Fs people over, right?

Maybe I'm exaggerating. I would love to hear your thoughts on this.

reply

*

Richard Menon (@bluentweb) - December 28th, 2009 at 2:56 am PST

Good one… also before creating account on social networking sites we should go through to all privacy policy, security terms and condition; and don't provide very personal information on it.

reply

*

Andre H - December 28th, 2009 at 3:01 am PST

as mentioned above. techcrunch uses facebook connect.

From the facebook connect website:

Facebook Connect is a powerful set of APIs for developers that lets users bring their identity and connections everywhere. Developers can access a user's:

Identity: name, photos, events, and more.

Social Graph: friends and connections.

Stream: activity, distribution, and integration points within Facebook, like stream stories and Publishers.

reply

*

curtis earl - December 28th, 2009 at 3:12 am PST

growing up, i've always wanted a solid state society. what my fantasy world didn't account for was the sheer ignorance of the sheeple. the average person doesn't seem to care about security until someone buys a house in their name. a close friend who happens to be a hiring manager says that she sends fake friend requests to interviewees ALL THE TIME. The people accept the requests and she trolls thru their personal information and then fact checks them in job interviews. i've begun the great PII purger. I've started eliminating my social sites. I deal with sites via a handle which never correlates with my actual identity. Some people think they do that already, then they look int the commenting options and log into this site with their FB.

reply

o

SirDobermann - December 28th, 2009 at 4:57 am PST

@curtis earl

perfectly true – what I never understood was how people can be so stupid to put their puzzle

pieces over several social networks – plus the info in network 1 about the ID in network 2 …

so I often found the city of a person in 1 and the correct first and last name in 2 – all I had to do was looking into the official online telephone book and I had their address and tel. number.

when I told them I had their phone number they were shocked :-D

well, I'm not the mean kind of person, I just do this to help them to become awake and alert, but not everyone is as friendly as I, so I told them to take out their correct names and cities

they should do like I've been doing all those years : use nicknames and never use PII

if they really want to become p e r s o n a l friends with s.o., they should either use email or mobile or traditional telephone

your "buy a house" idea once kind of happened to a CTF of mine (chat and tel. friend)

she recieved a letter from a mail+internet order co. asking when they should deliver the $23.000 luxury livingroom interior to her home :-D

someone she had been communicating with and met originally in a major "chat" program installed a customer account in her name…

reply

*

kevin - December 28th, 2009 at 4:13 am PST

A nice article after a long time about social sites…

I think most of us want to be known on the world wide web and also they wants to know the other prosepective about diiferent things and ideas…that's why theses social networking sites are growing up…But side by side there are certain things that matters as mentiones in the article"Privacy Theater"…

Really a good one…

reply

*

Ian (@uid0) - December 28th, 2009 at 5:12 am PST

One thing that a lot of folks don't know about Facebook is that Private Investigators and Attorneys/ Law Enforcement can get facebook accounts that do not adhere to the privacy restrictions — which leads me to tell people that if you don't want it discovered, don't put it online in the first place.

reply

*

Paramendra Kumar Bhagat

Paramendra Kumar Bhagat - December 28th, 2009 at 6:31 am PST

Digital ID issues will only become more acute.

reply

o

Tyler Gillies

Tyler Gillies - December 28th, 2009 at 6:36 am PST

I think digitial id is in its infancy and over the next coming years we will see a lot of reform in this area

reply

*

Tyler Gillies

Tyler Gillies - December 28th, 2009 at 6:33 am PST

Personally, I understand that I have no clue about the ethics of the company I give me data to, and I assume that all of it will eventually become public. If I consider information “private” i simply don’t put it on the internet. Although the one exception to this is credit card/banking information. I expect these people to hold to a higher standard.

reply

*

Jake - December 28th, 2009 at 7:43 am PST

“Users see worms on MySpace and viruses on Facebook, but not on Hotmail — because they defend against cross-site-scripting attacks. Users find malware distributed on Slide, but not on Wikipedia — because they filter content aggressively. Users are blocked by DDoS attacks and DNS attacks on Twitter — but Amazon stays up because they can react in real-time.”

Completely inaccurate. HOTMAIL is immune to worms and viruses because they “defend against XSS attacks”? What the hell?

reply

*

Brian Norgard (@briannorgard) - December 28th, 2009 at 8:05 am PST

Brilliant piece.

reply

*

Adam Boalt (@boalt) - December 28th, 2009 at 9:11 am PST

Excellent article. I expect privacy issues to be one of the major social media themes of 2010, especially as Facebook continues to look for ways to profit off of user’s data.

reply