

Bringing Security and Privacy to Where the Wild Things Are



Runa A. Sandvik // @runasand

About me

Things you knew and things you didn't

- **From Oslo, Norway**
- **Tested pens in London, UK**
- **Worked for The Tor Project**
- **And Freedom of the Press Foundation**
- **Currently freelancing**

**What does this have to do
with IoT and mobile?**

Back in 2010

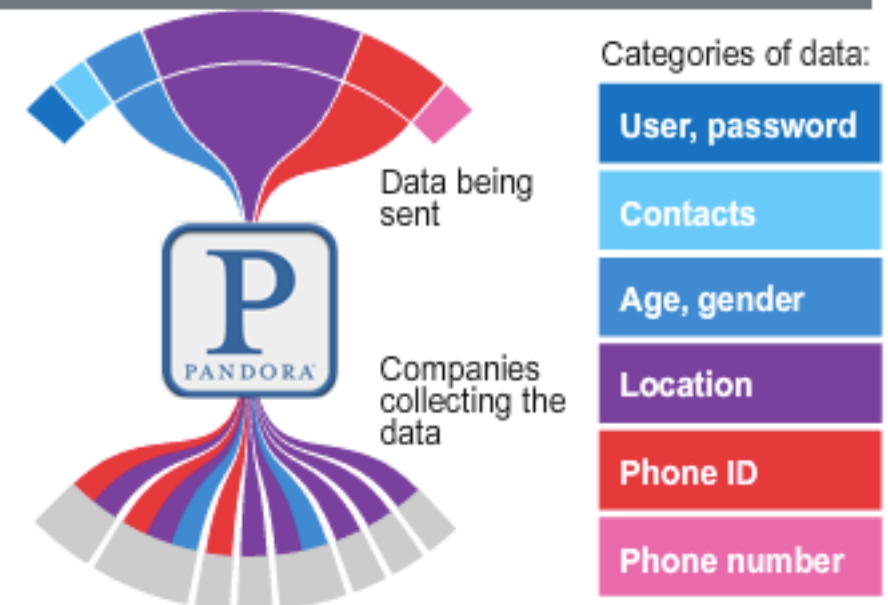
From the WSJ



What we found on one app

The iPhone version of music app Pandora sent information to eight trackers. It sent location data to seven of these, a unique phone ID to three and demographic data to two.

[Click to explore data on all the apps](#)



Two years later

Bullseye from 1,000 yards: Shooting the \$17,000 Linux-powered rifle

ARM CPUs, lasers, and Wi-Fi make firing this weapon an experience like no other.

by Lee Hutchinson - Mar 31, 2013 9:00pm EDT

[Share](#)

[Tweet](#)

444



Just the other day

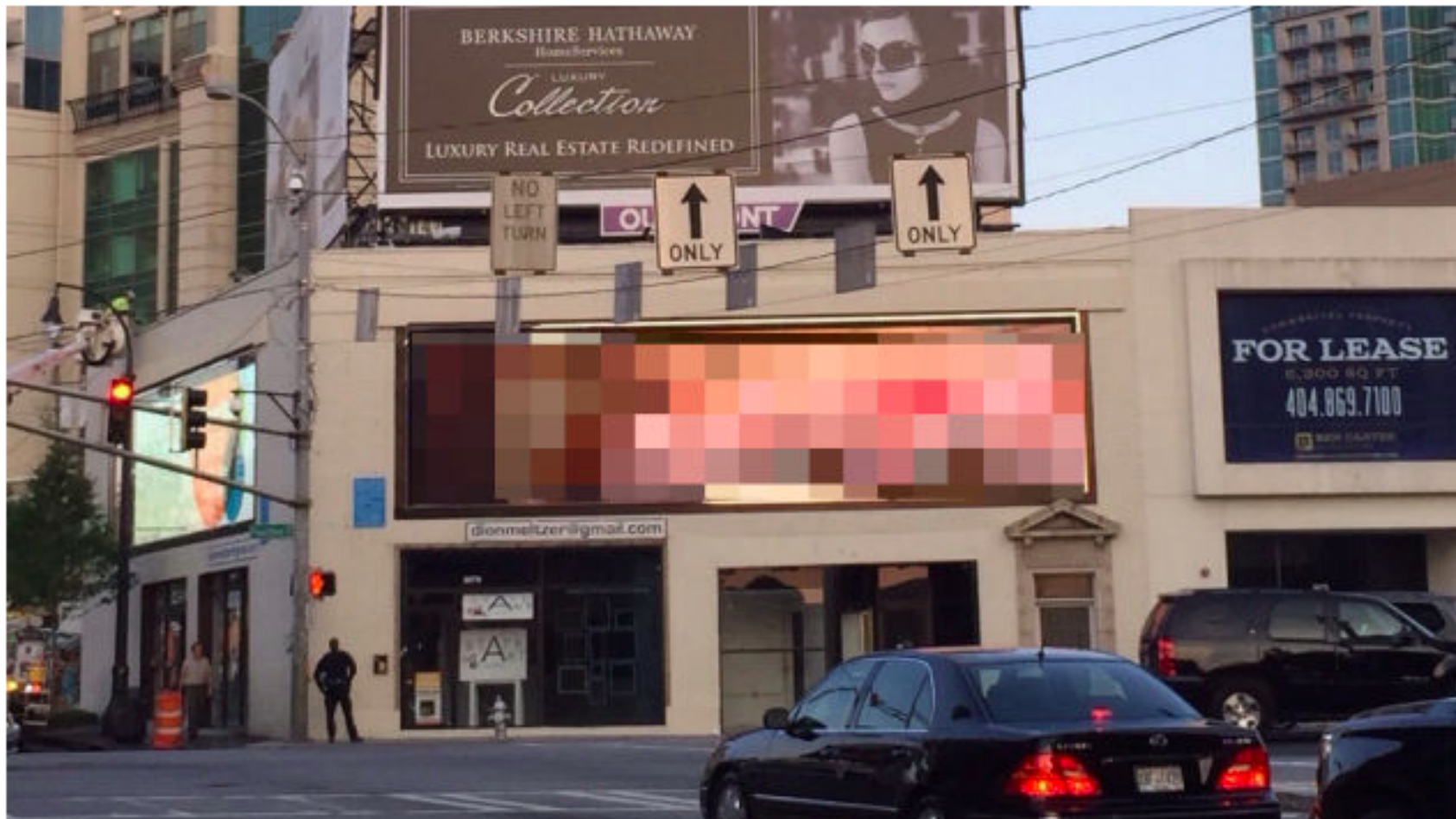
FBI and Homeland Security Respond to Shocking Goatse Bomb in Atlanta



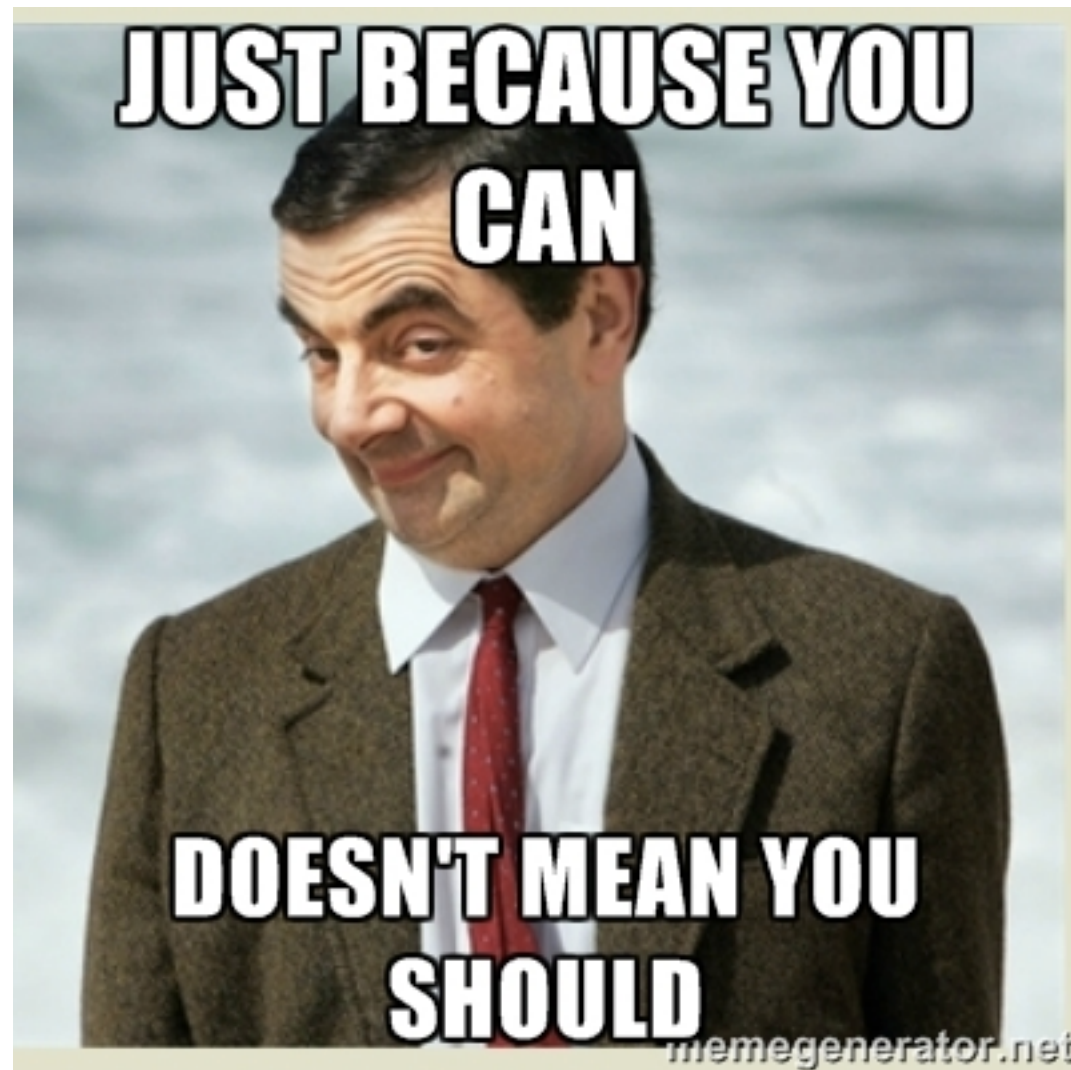
Sam Biddle

Filed to: GOATSE 5/15/15 2:35pm

180,924 🔥 50 ★ ⌵

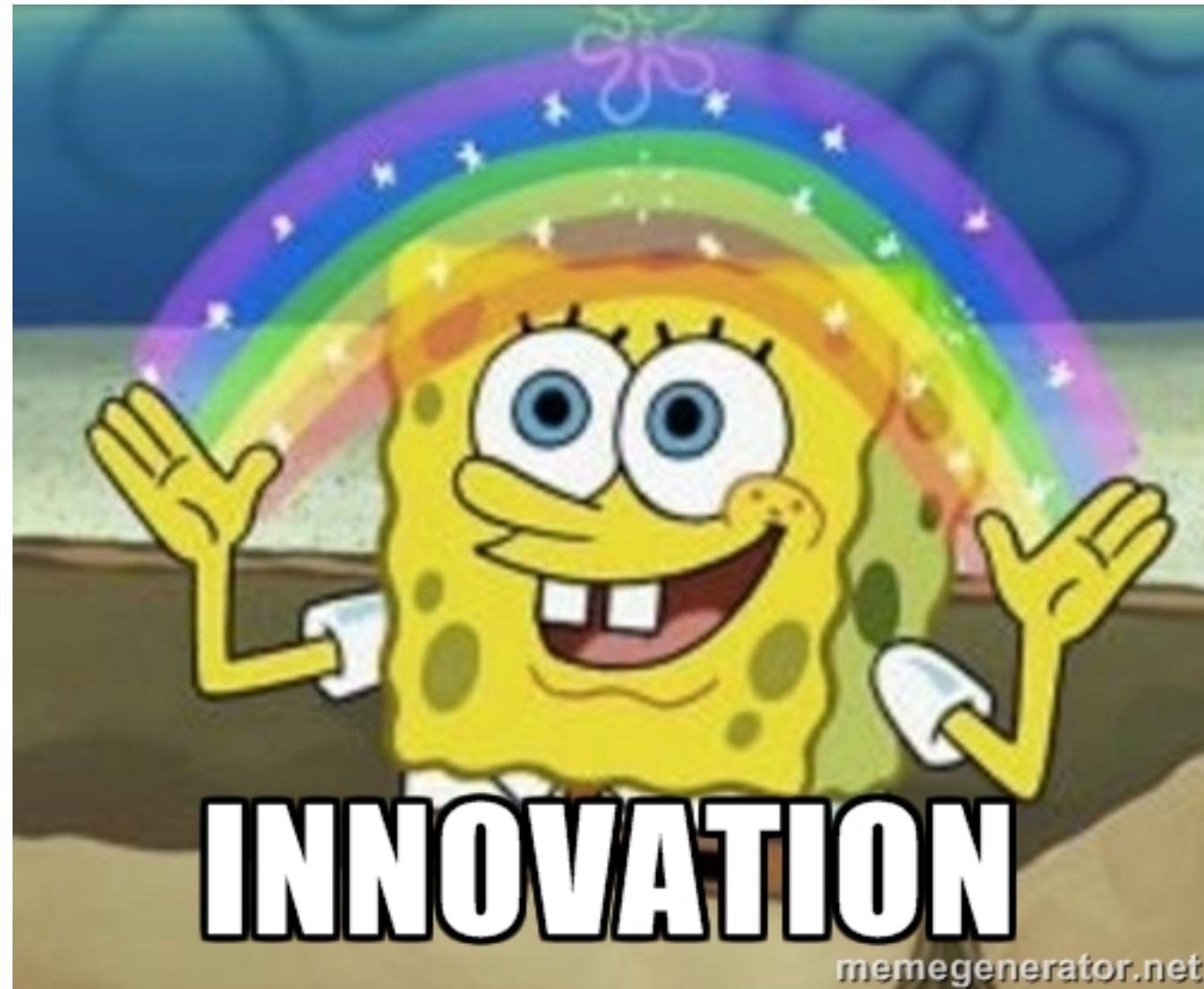


Something to keep in mind



So why do we do it?

Innovation

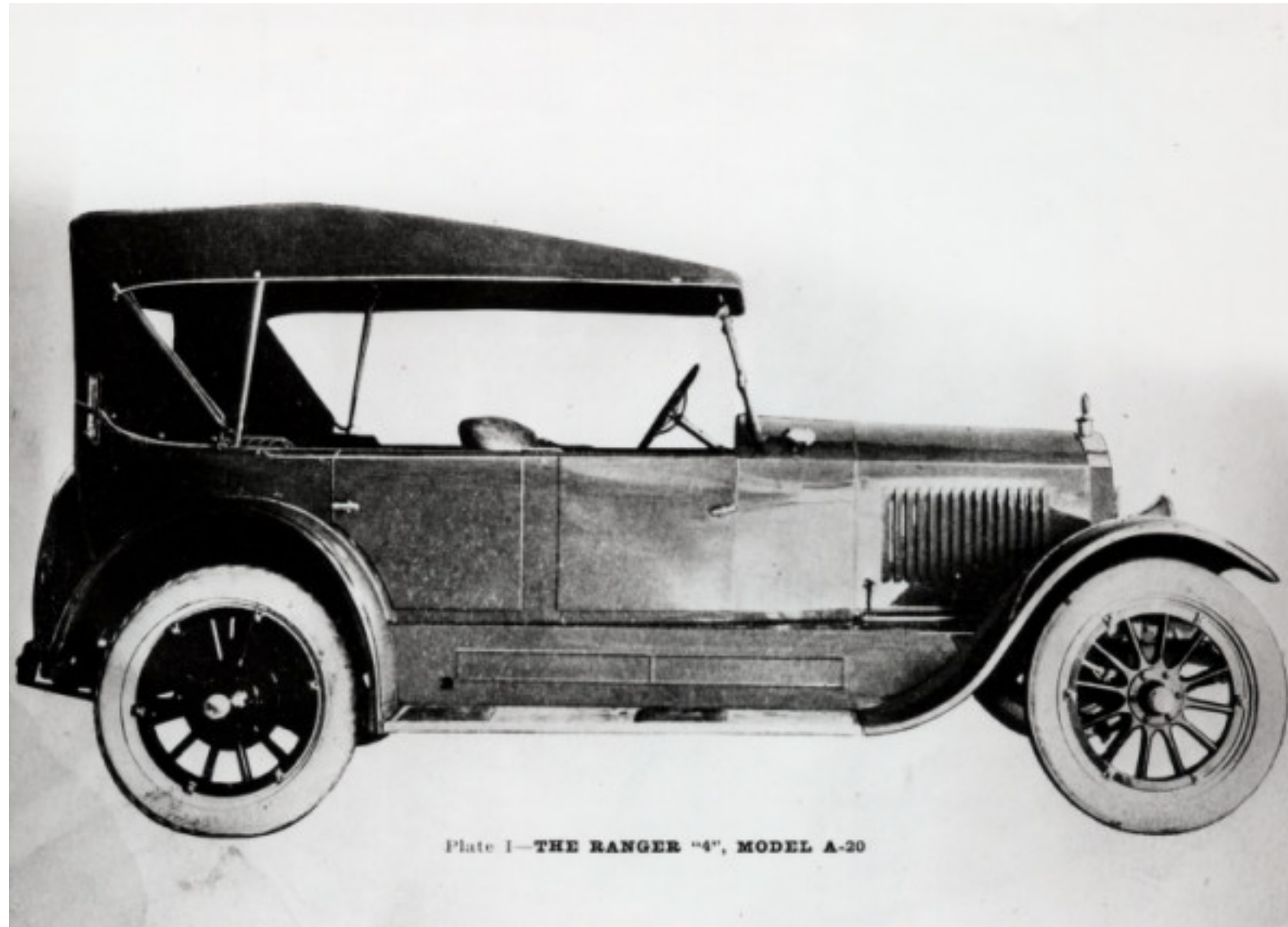


And money too



Managing expectations



Creating that baseline



And building on it



Dear journalists

Google  

Web News Shopping Videos Images More ▾ Search tools

About 3,960,000 results (0.42 seconds)

NSA-Proof? Super-Secure Blackphone Shipping by July ...

www.nbcnews.com/.../nsa-proof-super-secure-blackphon... ▾ NBCNews.com ▾

Jun 16, 2014 - If you wish your smartphone had more security and privacy features, you might soon be switching phones: pre-orders for the Blackphone, ...

'NSA-Proof' Email ProtonMail Launching Mobile App - Forbes

www.forbes.com/.../nsa-proof-email-protonmail-launching-mobil... ▾ Forbes ▾

Aug 1, 2014 - ProtonMail, the email service which looks and feels like Gmail but is, according to its CERN particle physicists developers, the closest thing to ...

NSA-proof - VentureBeat

venturebeat.com/.../fundraiser-to-support-nsa-proof-email-gets-off-to-a-r... ▾

Jun 21, 2014 - ProtonMail, an encrypted email service that advertises itself as “**NSA-proof**,” launched to much acclaim about a month ago. Since then, the ...

German 'NSA-proof' private server raises \$1mn ... - RT.com

rt.com/news/163968-nsa-proof-server-crowdfunding/ ▾ RT ▾

German 'NSA-proof' private server raises \$1mn crowdfunding in 89 minutes. Published time: June 05, 2014 18:36. Edited time: June 06, 2014 23:25. Get short ...

Dear hackers



VENOM

VIRTUALIZED ENVIRONMENT NEGLECTED OPERATIONS MANIPULATION

Discovered by Jason Geffner, CrowdStrike Senior Security Researcher

We can do better

Data Retention

This section details what data OTR.im can see and can not see on this Jabber server.

First of all, this server is setup with [full disk encryption](#) (FDE) so all that we store is only on an encrypted disk. We use a [LUKS](#) device for this. Security is disabled on the Jabber server, even error logs.

In case of a seizure, if the server is powered off, the FDE will protect all data. If the server is kept online, see the *What we can see?* section below

What we CAN see?

- Your username and [SHA1](#) hash of the password are stored on the server.
- [vCard](#) if you supply one.
- Your IP address. To avoid this, use our Tor hidden service.
- Offline messages. Any messages you send to an offline contact will be stored encrypted on the server until the contact shows up.
 - Encrypted content (OTR).
 - Destination contact address.
 - Timestamp of the message.
- Your roster. For each contact:
 - Jabber address (ex: [keith@jabber.boozallen.com](#))
 - Name of the contact (if set)
 - Group (if any)

What we DO NOT see?

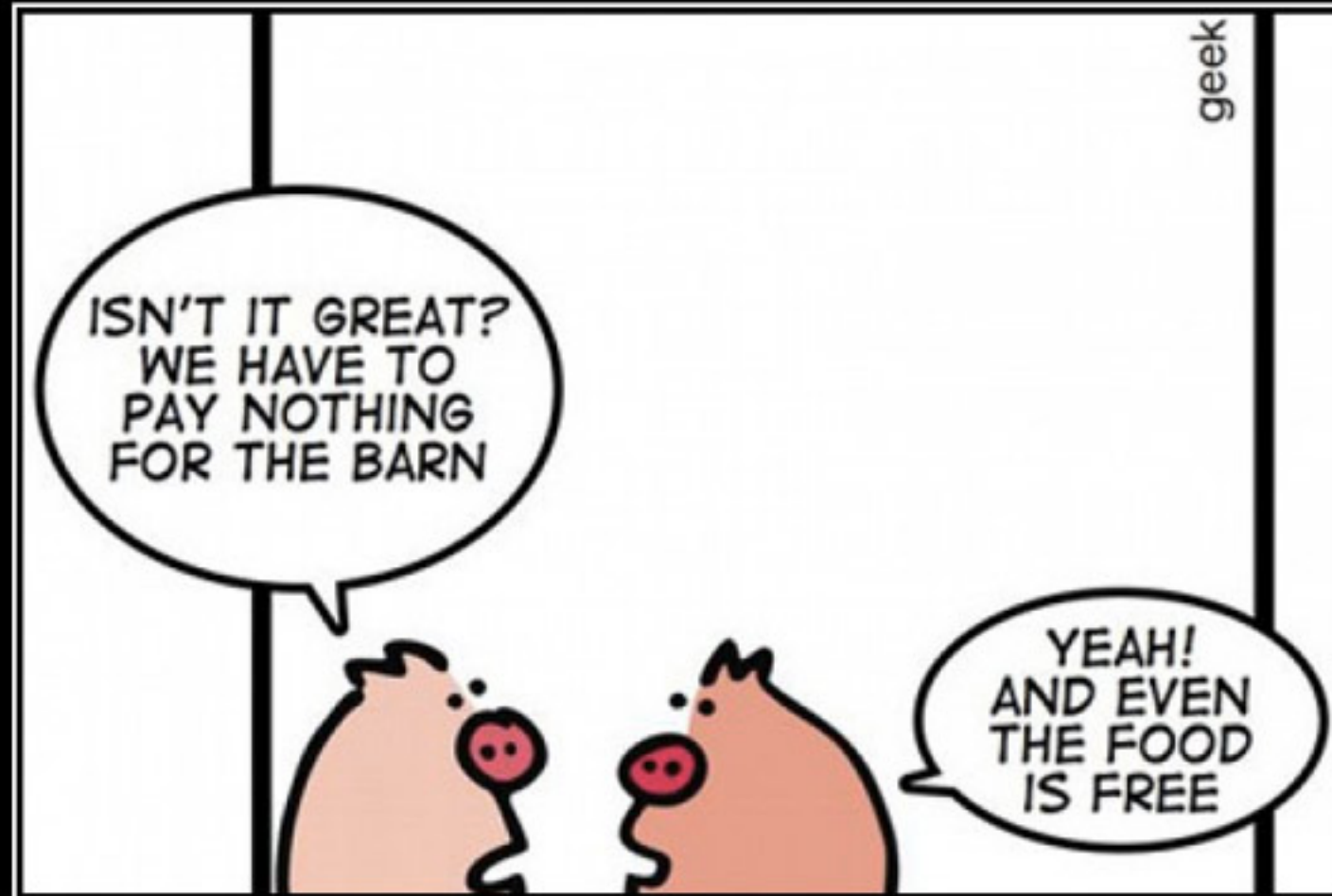
- Message content. Mandatory OTR makes it that we can't read content.
- No logs thus nothing our prosody server could usually tell us.
- We don't keep any timing metadata such as when you connect or disconnect.

Security versus privacy

While in London



Data has value



FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.

Yes, really

If you're one of the 117 million people who've shopped at RadioShack in recent years, your data is up for auction on Thursday.

This isn't a few hackers trying to cash in. It's the bankrupt electronics retailer [trying to raise money to pay off creditors](#).

Not just \$\$\$

Dating website hack leaks data of 4M users

Jacob Pramuk | @jacobpramuk

2 Hours Ago



Personal data from about 4 million profiles on a popular dating website has leaked after a hack, [Britain's Channel 4 reported Thursday](#).

People will do crazy things

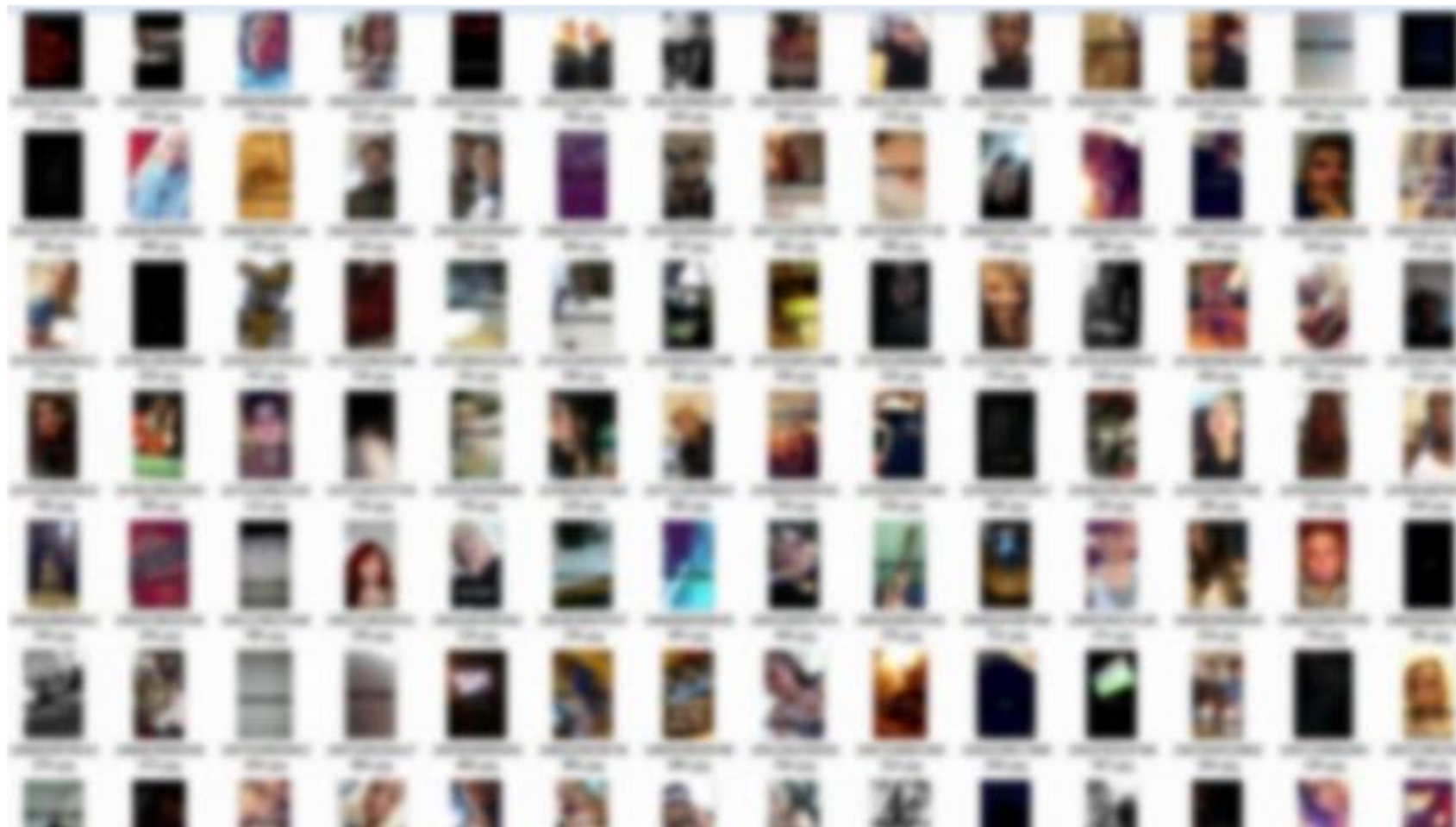
Snapchat: Those Thousands of Leaked Nudes Are Your Fault, Not Ours



Jay Hathaway

Filed to: SNAPCHAT 10/10/14 1:20pm

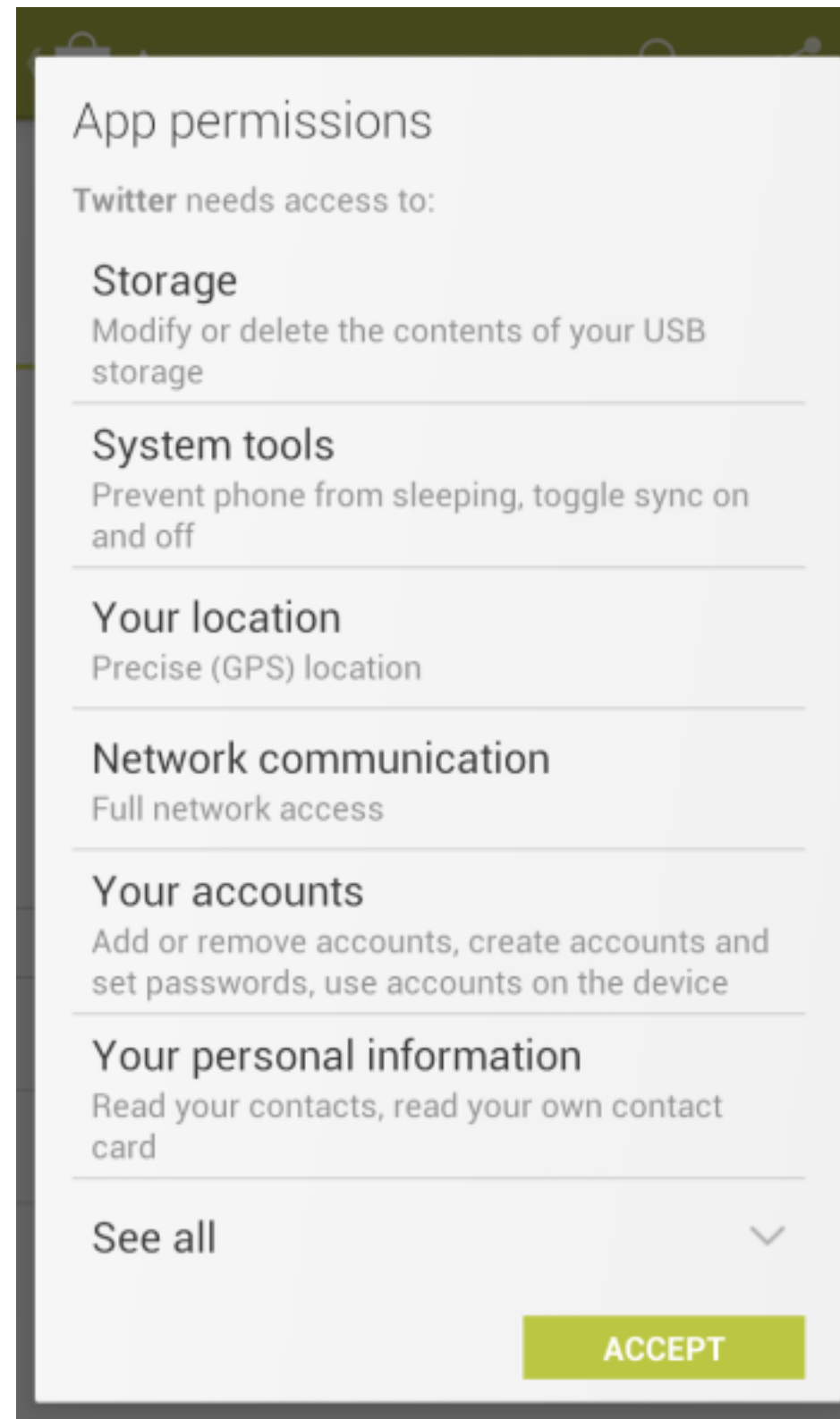
165,485 🔥 3 ★ ⌵



Rules of the road



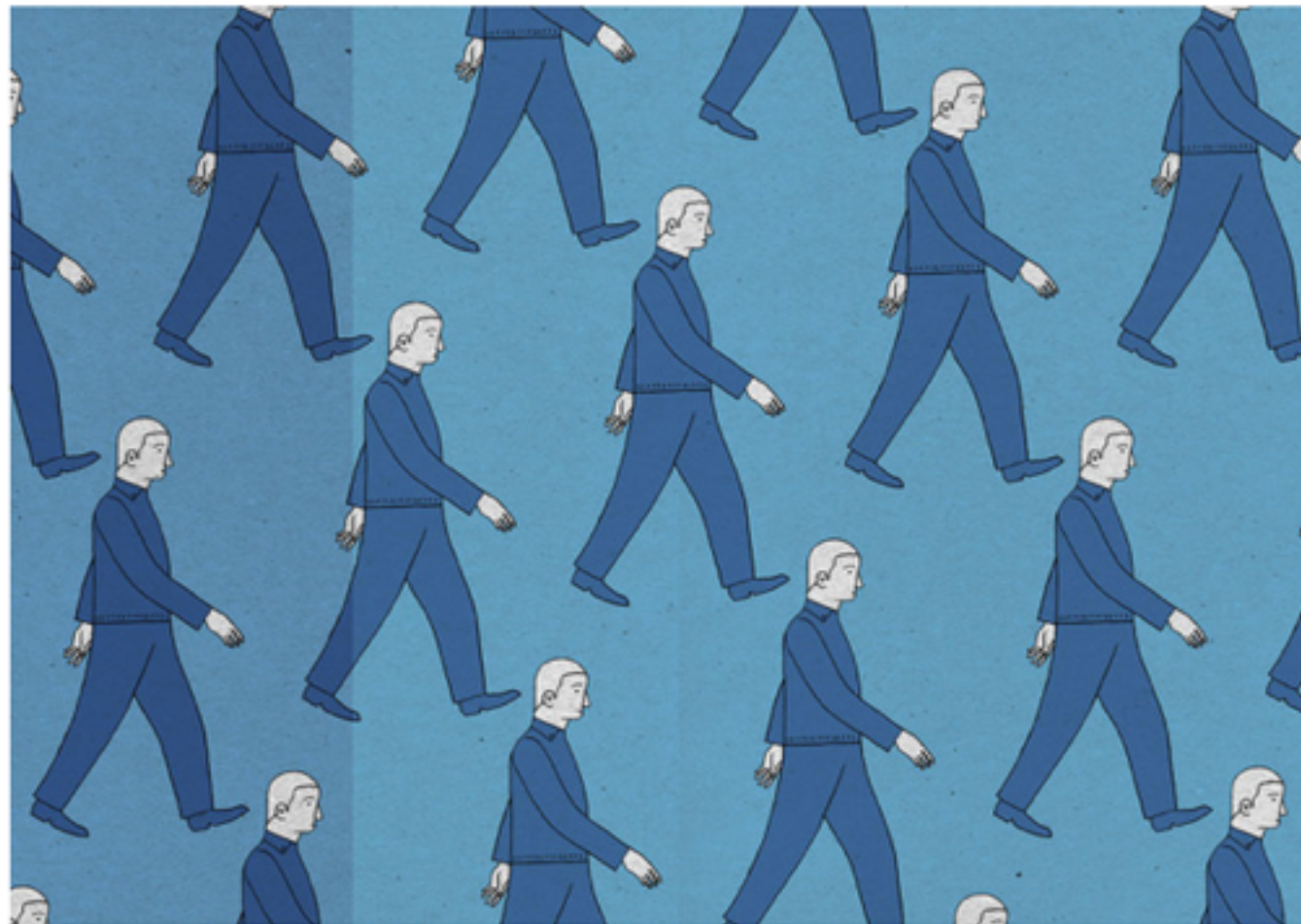
Transparency is key



When pigs fly

ANDY GREENBERG 10.31.14 12:31 PM

WHY FACEBOOK JUST LAUNCHED ITS OWN 'DARK WEB' SITE



Better late than never?



Chris Eng
@chriseng

Medical device security: "bake it in, don't bolt it on". Long known, but good to see FDA advocating for responsible practices. [#srcbos](#)

5/28/15, 3:36 PM

1 RETWEET 1 FAVORITE



Better late than never?



Chris Eng
@chriseng

"Vulnerabilities will emerge throughout the lifetime of a product." Again, infosec ppl know this. Good to see FDA understanding. [#srcbos](#)

5/28/15, 3:38 PM



All you have to do is ask



Chris Eng
@chriseng

"Introduce security requirements into contract language." Yes.

[#srcbos](#)

5/28/15, 3:40 PM

2 RETWEETS 1 FAVORITE

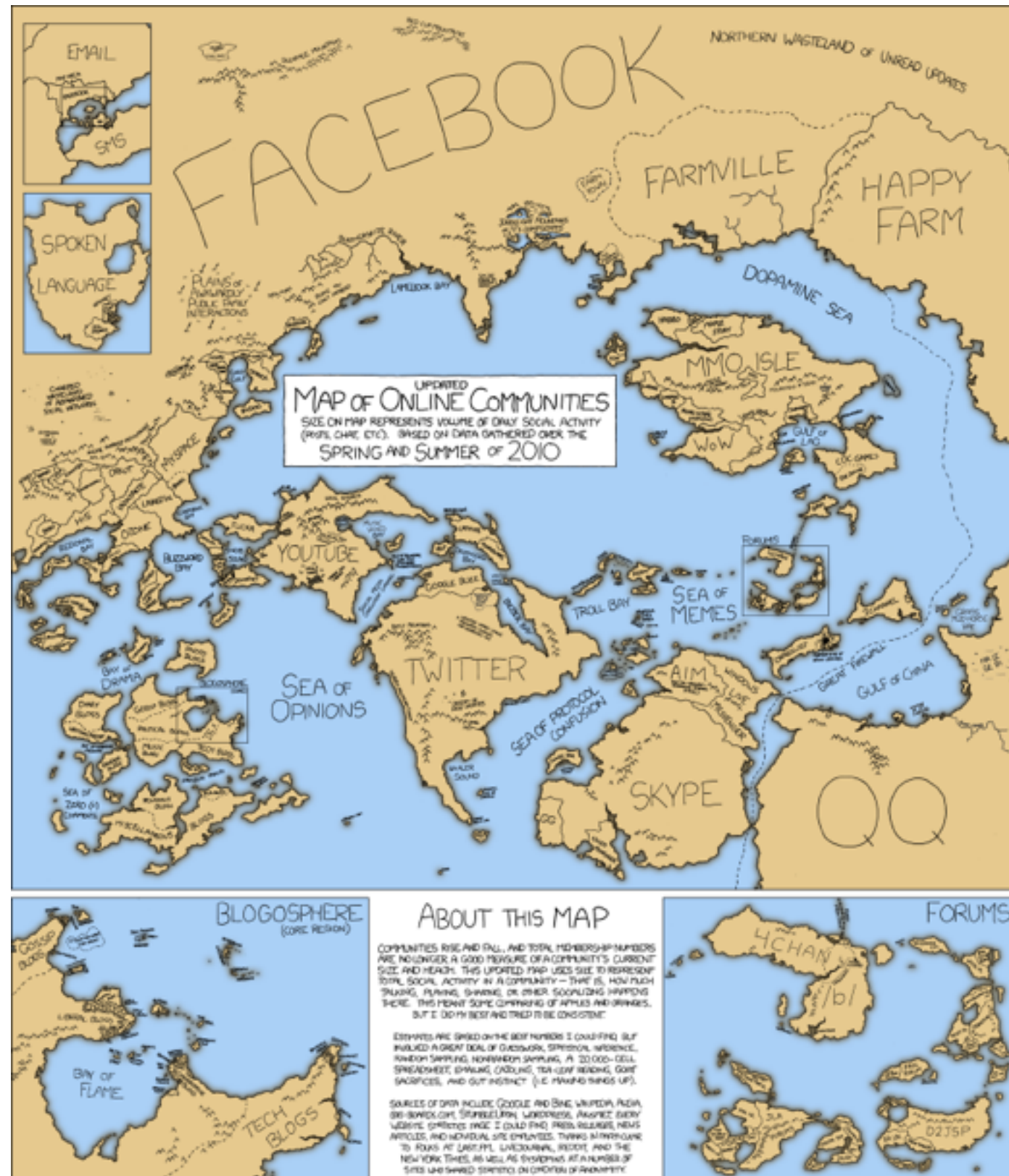


Where do we go from here?

The real question is...

How do you educate people?

No privacy utopia



We can do what we do best

WHEN IOT ATTACKS: HACKING A LINUX-POWERED RIFLE

TrackingPoint is an Austin startup known for making precision-guided firearms. These firearms ship with a tightly integrated system coupling a rifle, an ARM-powered scope running a modified version of Linux, and a linked trigger mechanism. The scope can follow targets, calculate ballistics and drastically increase its user's first shot accuracy. The scope can also record video and audio, as well as stream video to other devices using its own wireless network and mobile applications.

In this talk, we will demonstrate how the TrackingPoint long range tactical rifle works. We will discuss how we reverse engineered the scope, the firmware, and three of TrackingPoint's mobile applications. We will discuss different use cases and attack surfaces. We will also discuss the security and privacy implications of network-connected firearms.

Stay classy



Runa A. Sandvik

@runasand

+ Follow

Hey @pastebin, users should not have to pay for HTTPS. Please enable this for everyone?



RETWEETS

62

FAVORITES

15



4:39 PM - 6 Jan 2014

Not everyone will want your help



Dan Tentler
@Viss

 Follow

The same sign company that not just yesterday told me "we don't want your help" was just on the news for being hacked.



RETWEETS

17

FAVORITES

20



10:46 AM - 14 May 2015

Be responsible

SECURITY 5/20/2015 @ 5:54AM | 424 views

Gun Ammo, Bomb Supplies, Hacked Cars And Planes: Dangerous Tweets For A Security Researcher

+ Comment Now + Follow Comments

Though the issues Chris Roberts, [alleged plane hacker](#) and co-founder of [security](#) research firm One World Labs, has raised in recent weeks are bigger than just one man, looking through his past tweets provide all in the industry with a timely reminder of what maybe shouldn't be said in public, or even private, discussions.

It's not all about code

I Am The Cavalry

[About](#)[Domains](#)[Get Involved](#)[News & Blog](#)[Talks & Events](#)

I Am The Cavalry Advocates Automotive Cyber Safety

Join us in [encouraging the automotive industry to commit to cyber safety](#). At the annual DEF CON :
[Safety Framework \(PDF download\)](#) and calls for Automotive Industry adoption. Media outlets from across
security researchers to work together to ensure a safe future.



BuildItSecure.ly

[GOALS](#)[VENDORS](#)[BUGCROWD](#)[RESEARCH](#)

Our Goals for the "Internet of Things"

- 👁️ FOCUS effort towards crowd-funded, small commercial and bootstrapped vendors
- ♥️ BUILD partnerships and goodwill between IoT vendors and the security community
- ✓ COORDINATE efforts to incentivize security researchers for reporting vulnerabilities
- 📝 CURATE informational resources to help educate vendors on security best practices
- 👤 PRESENT research at relevant events and be a point of contact for press inquiries

Thanks!
Questions?



Runa A. Sandvik // @runasand