ONLINE PRIVACY CONCERNS

(and what we can do about it)

Phil Cryer

StlLinuxUG

June 20 , 2013

Phil Cryer

Phil Cryer

better known online as...

@FAK3R

Phil Cryer

OPEN SOURCE TECHNOLOGIST

better known online as...

@FAK3R

Phil Cryer

OPEN SOURCE TECHNOLOGIST

INFOSEC SPEAKER+RESEARCHER

better known online as...

@FAK3R

Phil Cryer

OPEN SOURCE TECHNOLOGIST

INFOSEC SPEAKER+RESEARCHER

PRIVACY ADVOCATE

better known online as...

@FAK3R

"With social media, users' vanity has trumped previously held mores concerning privacy"

me, 2011

http://urania-josegalisifilho.blogspot.com/2012/06/interview-with-willian-gibson-by-larry.html

People's data on social networks becomes permanently shared.

So what will companies do to monetize all of this data they collect?

Use it to better target you with ads, of course.

To you, your social profile

To you, your social profile =

To you, your social profile = data

To you, your social profile = your data

But to the social media companies

But to the social media companies your data

But to the social media companies your data =

https://christian3200.files.wordpress.com/2011/04/moneyyyyy.jpg

http://cheezburger.com/View/2362193664

So, how much should people worry about the loss of online privacy?

Danah Boyd "People want to share. But that's different than saying that people want to be exposed by others."

Protecting privacy is about making certain that people have the ability to make informed decisions about how they engage in public. I do not think we've done enough.

That said, I am opposed to approaches that protect people by disempowering them. I want to see approaches that force powerful entities to be transparent about their data practices. And I want to see approaches that put restrictions on how data can be used to harm people.

WSJ.com

http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html

Chris Soghoian "...we now regularly trade our most private information for access to social-networking sites and free content"

The dirty secret of the Web is that the 'free' content and services that consumers enjoy come with a hidden price: their own private data.

Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.

WSJ.com

http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html

Whose Life Is It Anyway? Consumers are learning their data is a kind of currency.

http://www.adweek.com/news/advertising-branding/whose-life-it-anyway-137537

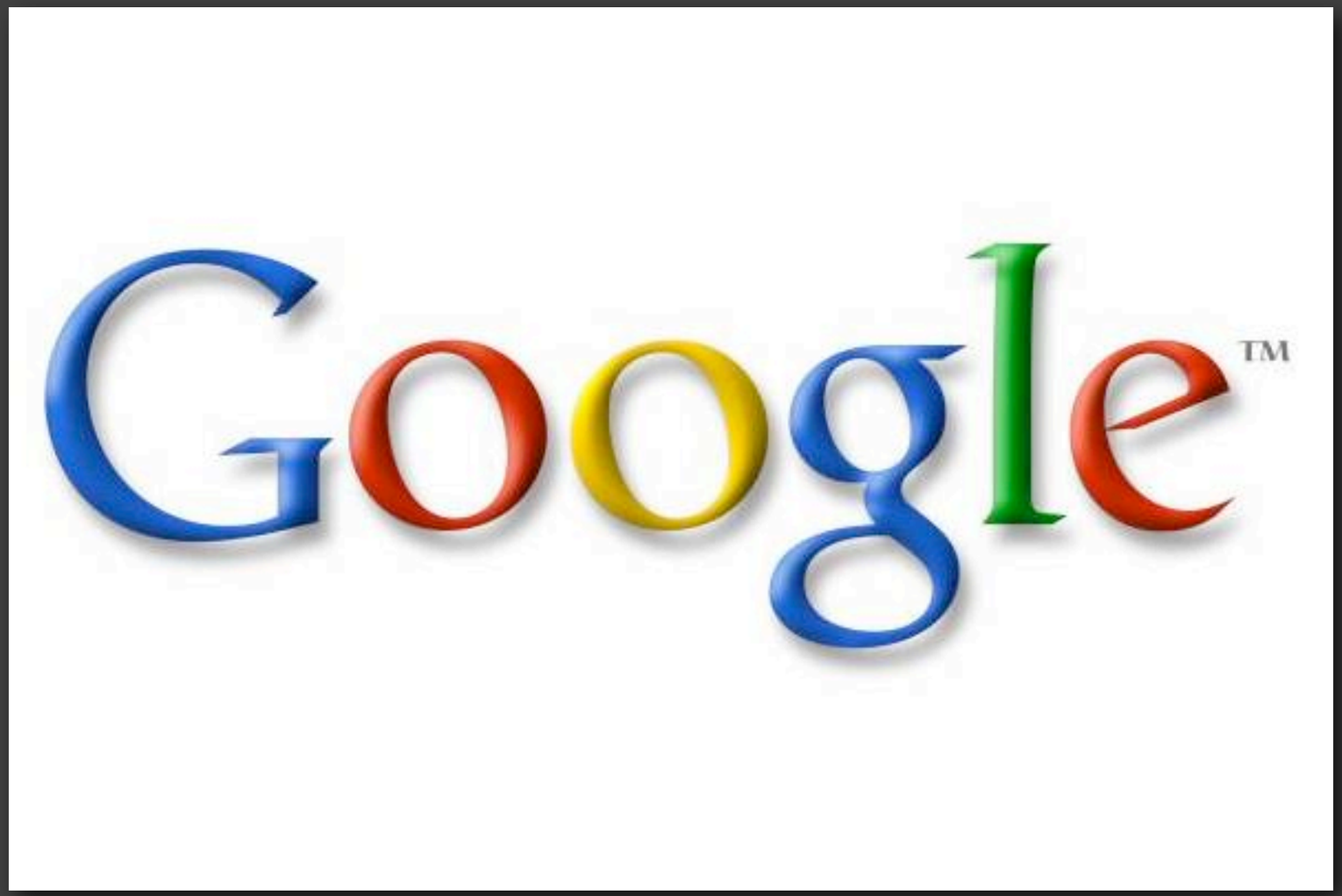
Whose Life Is It Anyway? Consumers are learning their data is a kind of currency.

Each year, companies in the U.S. spend more than $2 billion on third-party consumer data, according to Forrester Research. [...] growing at such a fast clip that the World Economic Forum and other futurists have called personal data the "new oil."

http://www.adweek.com/news/advertising-branding/whose-life-it-anyway-137537

COMPANIES' 'FREE' SERVICES COME AT THE COST OF YOUR PRIVACY

Could your privacy be bought from you?



http://www.forbes.com/sites/kashmirhill/2012/02/09/your-online-privacy-is-worth-less-than-a-six-pack-of-marshmallow-fluff

Google [...] wants “panelists” for a program called Screenwise who will add a browser extension in Chrome “that will share with Google the sites you visit and how you use them” — information that Google will study in order to improve its products and services.

http://www.forbes.com/sites/kashmirhill/2012/02/09/your-online-privacy-is-worth-less-than-a-six-pack-of-marshmallow-fluff

What's in it for you? Up to $25 in gift cards. [..] a $5 Amazon.com Gift Card code instantly when you sign up and download the Google Screenwise browser extension. [...] $5 Amazon.com Gift Card codes every three months for staying with it. It's our way of saying **"Thank you"**

http://www.forbes.com/sites/kashmirhill/2012/02/09/your-online-privacy-is-worth-less-than-a-six-pack-of-marshmallow-fluff

$25 USD **per year**

http://www.forbes.com/sites/kashmirhill/2012/02/09/your-online-privacy-is-worth-less-than-a-six-pack-of-marshmallow-fluff

“New research finds people fork over $5,000 worth of personal information a year to Google in exchange for access to its “free services” such as Gmail and search. While many view this as a fair trade, privacy experts say the Internet giant’s latest plan to pool user data from its various sites make it less so”

http://blogs.smartmoney.com/advice/2012/01/25/who-would-pay-5000-to-use-google-you

IF YOU'RE NOT PAYING FOR THE PRODUCT, YOU ARE THE PRODUCT

- 1.1 billion monthly active users
- 751 million daily active users of mobile products
- More than 65% login daily (655 million)
- Average user has 130 friends

http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

- More than 70 languages available on the site
- Over 300,000 users helped translate the site through the translations application
- 79% of users are outside of the US/Canada

http://newsroom.fb.com/content/default.aspx?NewsAreaId=22


facebook

```
$ _
```


facebook


```
$ curl -s http://graph.facebook.com/4 | python -mjson.tool
{
    "first_name": "Mark",
    "gender": "male",
    "id": "4",
    "last_name": "Zuckerberg",
    "link": "http://www.facebook.com/zuck",
    "locale": "en_US",
    "name": "Mark Zuckerberg",
    "username": "zuck"
}
```

http://graph.facebook.com/4

Mark Zuckerberg starts Facebook at 19 while still at Harvard, but early messages don't show a strong interest in privacy...

An early instant message session with a friend...

Zuck: Yeah so if you ever need info about anyone at Harvard
Zuck: Just ask.
Zuck: I have over 4,000 emails, pictures, addresses, SNS
[Name Redacted]: What? How'd you manage that one?
Zuck: People just submitted it.
Zuck: I don't know why.
Zuck: They "trust me"
Zuck: Dumb f***s

https://en.wikiquote.org/wiki/Mark_Zuckerberg
http://articles.businessinsider.com/2010-09-13/tech/30033368_1_ims-mark-zuckerberg-facebook-ceo

Privacy no longer a social norm, says Facebook founder

"People have really gotten comfortable not only sharing more information ... with more people," he said. "That social norm is just something that has evolved over time."

http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

Facebook Privacy: A bewildering Tangle of Options

"To manage your privacy on Facebook, you will need to navigate through 50 settings with more than 170 options. Facebook says it wants to offer precise controls for sharing on the Internet."

https://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html

WEB PAGE ON FACEBOOK
SUBCATEGORY
PRIVACY SETTING OPTION

MAIN FACEBOOK ACCOUNT PAGE

SETTINGS PAGE

FACEBOOK ADS PAGE

PRIVACY SETTINGS PAGE

SUBCATEGORIES INCLUDE:

PERSONAL INFORMATION
bio, posts, photo albums

CONTACT INFORMATION
phone numbers, e-mail and physical addresses

FRIENDS, TAGS, CONNECTIONS
family, friends, activities and interests

APPLICATIONS AND WEB SITES
Facebook-enhanced Web sites

SEARCH
Facebook or public search results

BLOCK LIST
Blocked individuals

Facebook or third-party ads

PHOTOS
Each photo album created has its own settings

PERSONALIZED ADS Two additional settings not visible in the Privacy tab allow you to control how your information is shared and used with Facebook ads and third-party ads.

FRIENDS SHARING YOUR INFORMATION Even if you have changed all of your personal settings to private on Facebook, this tab allows your friends, even without their knowledge, to share your name, profile picture, gender and more with third- party Web sites and applications.

WHO CAN SEE YOU Most privacy settings come with five suboptions to decide who can see your personal

INSTANT PERSONALIZATION This setting allows some Facebook partners – currently Microsoft Docs, Pandora and Yelp – to customize their sites using

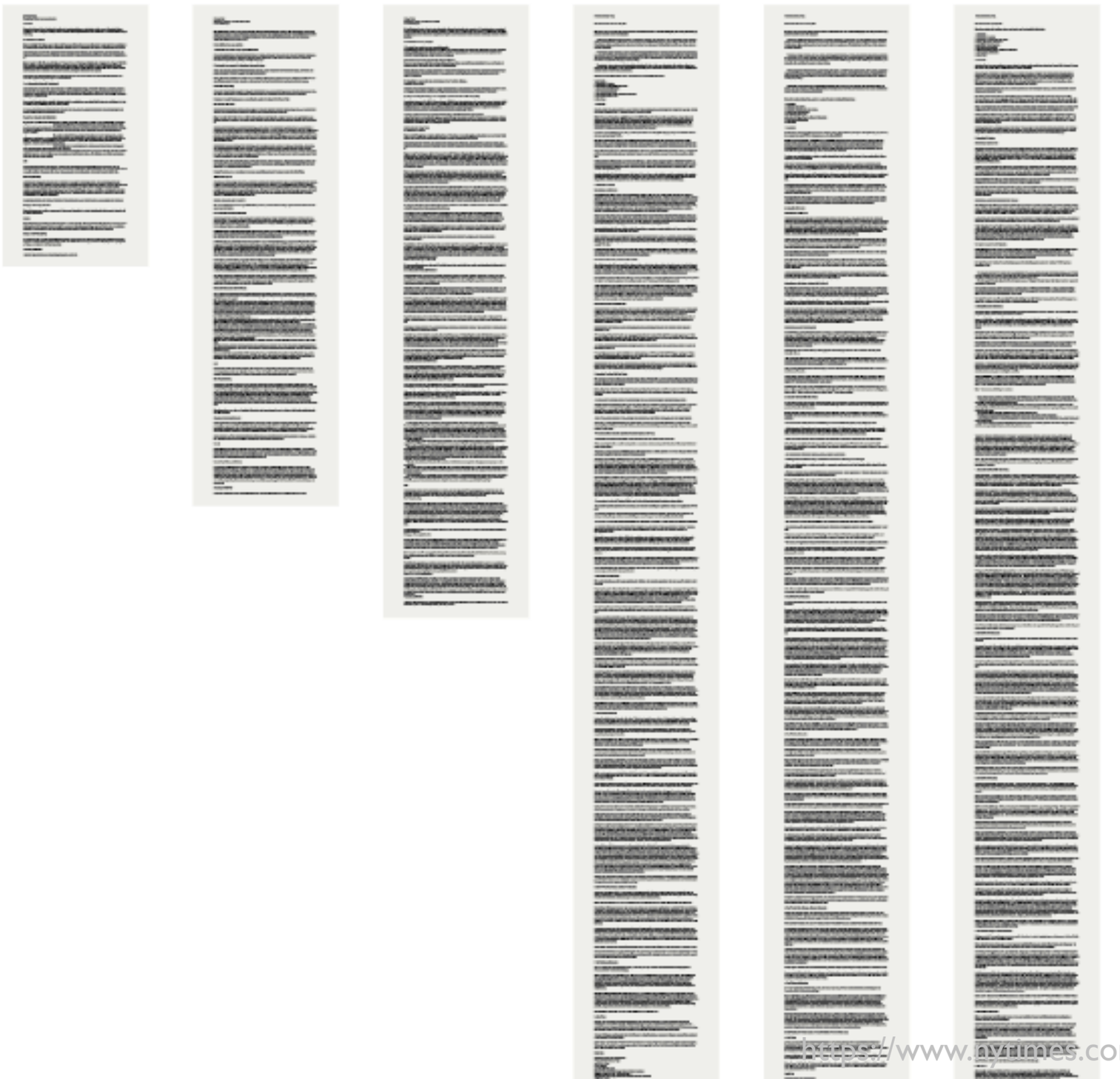
ALLOW YOUR FRIENDS TO SHARE:
Status updates
Website

The ever-expanding privacy policy

In the last five years Facebook's privacy policy has grown to 5,830 words today, from 1,004 in 2005. In addition, Facebook offers an in-depth Privacy FAQ page, with 45,000 words.

WORD COUNT OF FACEBOOK'S PRIVACY STATEMENTS

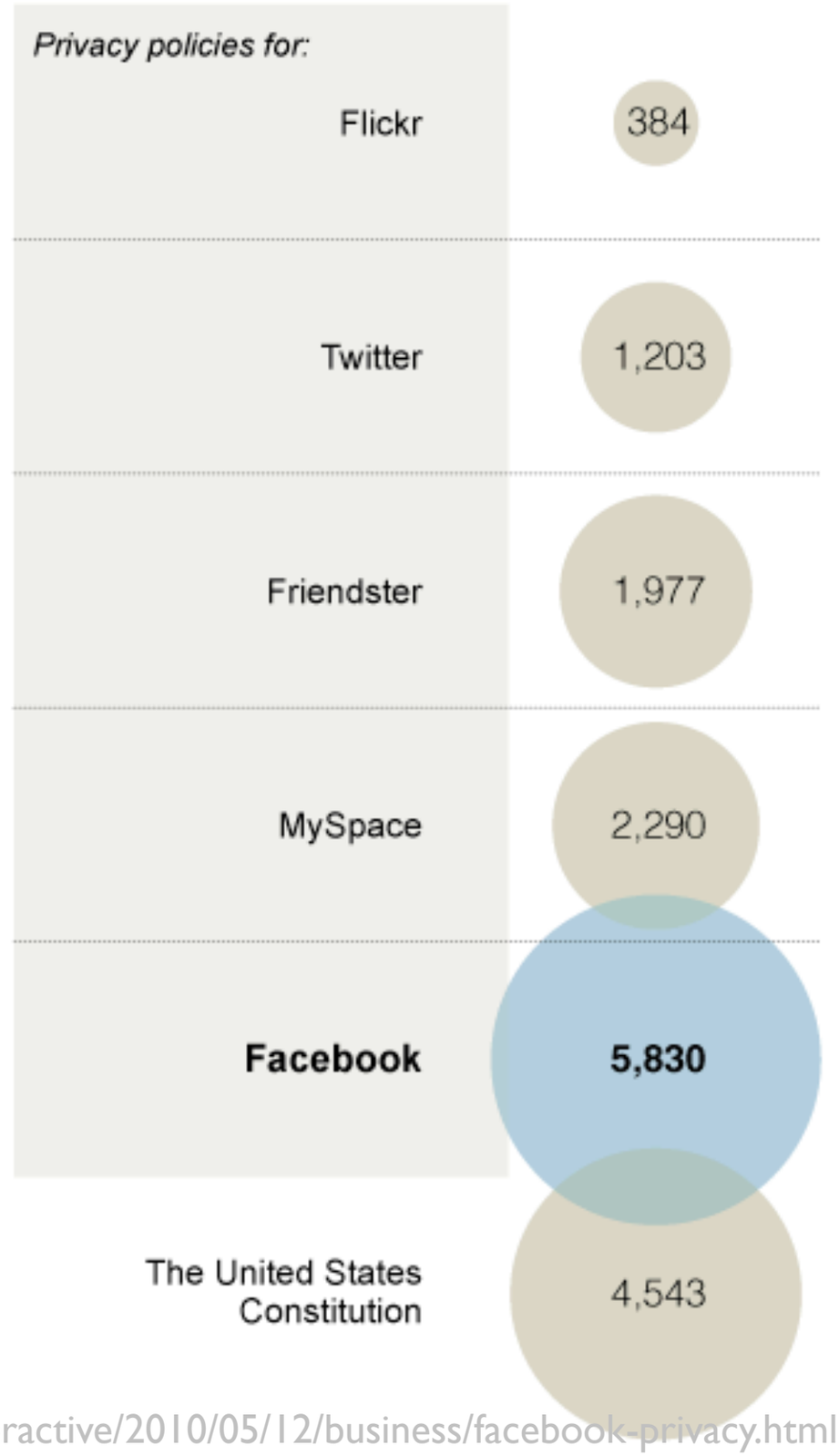
2005	2006	2007	NOV. 2009	DEC. 2009	2010
1,004	2,313	3,067	5,394	5,443	**5,830 words**

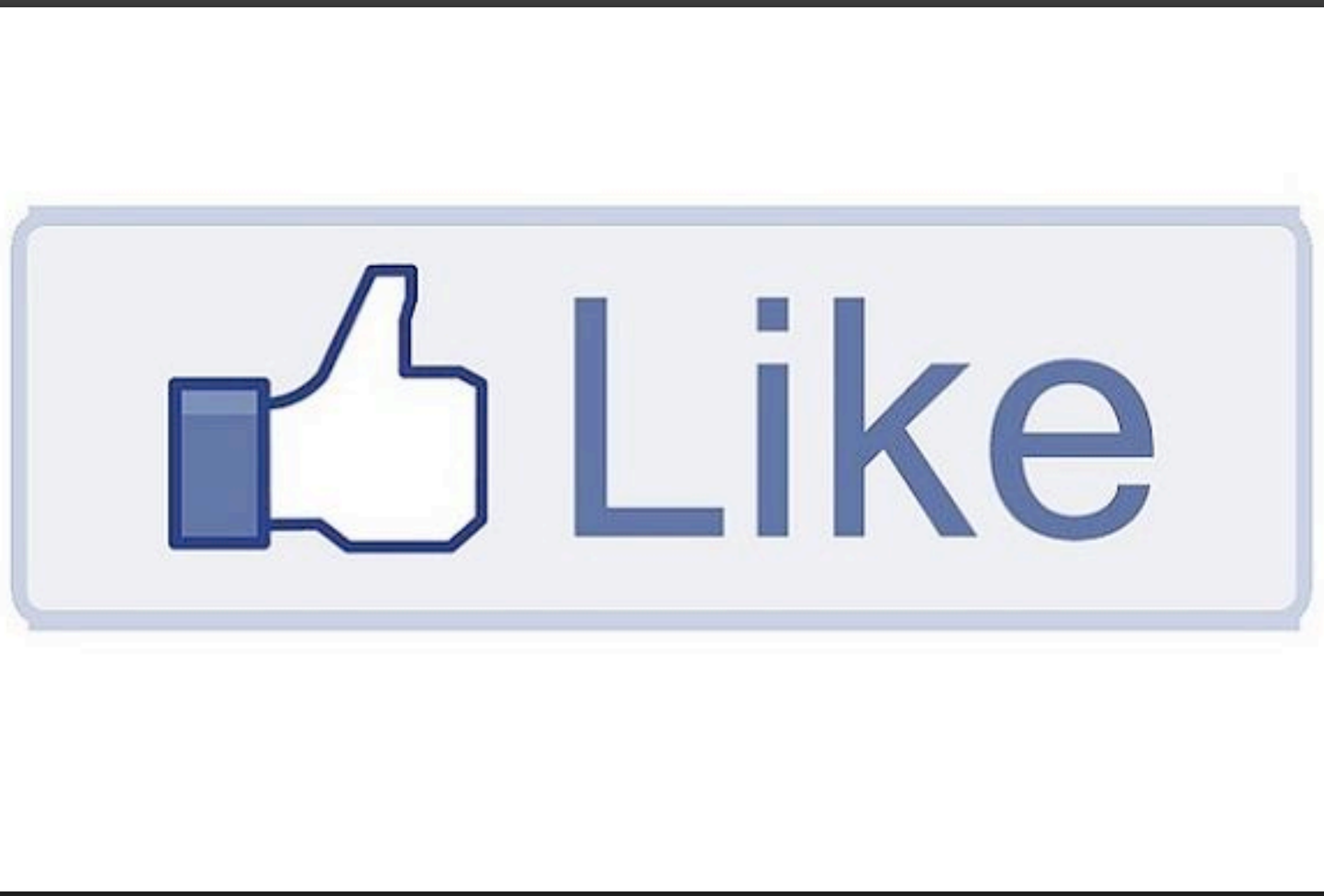


Longer than the Constitution

Facebook's 2010 privacy policy is longer than that of other social networks, even exceeding the United States Constitution, without the amendments.

WORD COUNTS





http://facebook.com

Chris Soghoian "Facebook's covert surveillance of your browsing activities on non-Facebook websites..."

Although consumers knowingly share information via Facebook, the privacy issues associated with that company are not related to the way consumers use it, but rather the other things the company does.

These include the tricks the company has pulled to expose users' private data to third-party app developers, the changing privacy defaults for profile data, as well as Facebook's covert surveillance of your browsing activities on non-Facebook websites, as long as a "Like" button is present (even if you don't click on it).

WSJ.com

http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html

ReadWriteWeb

Facebook has cut a deal with political website Politico that allows the independent site machine-access to Facebook users' messages, both public and private, when a Republican Presidential candidate is mentioned by name. The data is being collected and analyzed for sentiment by Facebook's data team, then delivered to Politico to serve as the basis of data-driven political analysis and journalism.

The move is being widely condemned in the press as a violation of privacy but if Facebook would do this right, it could be a huge win for everyone. Facebook could be the biggest, most dynamic census of human opinion and interaction in history. Unfortunately, failure to talk prominently about privacy protections, failure to make this opt-in (or even opt out!) and the inclusion of private messages are all things that put at risk any remaining shreds of trust in Facebook that could have served as the foundation of a new era of social self-awareness.

POLITICO

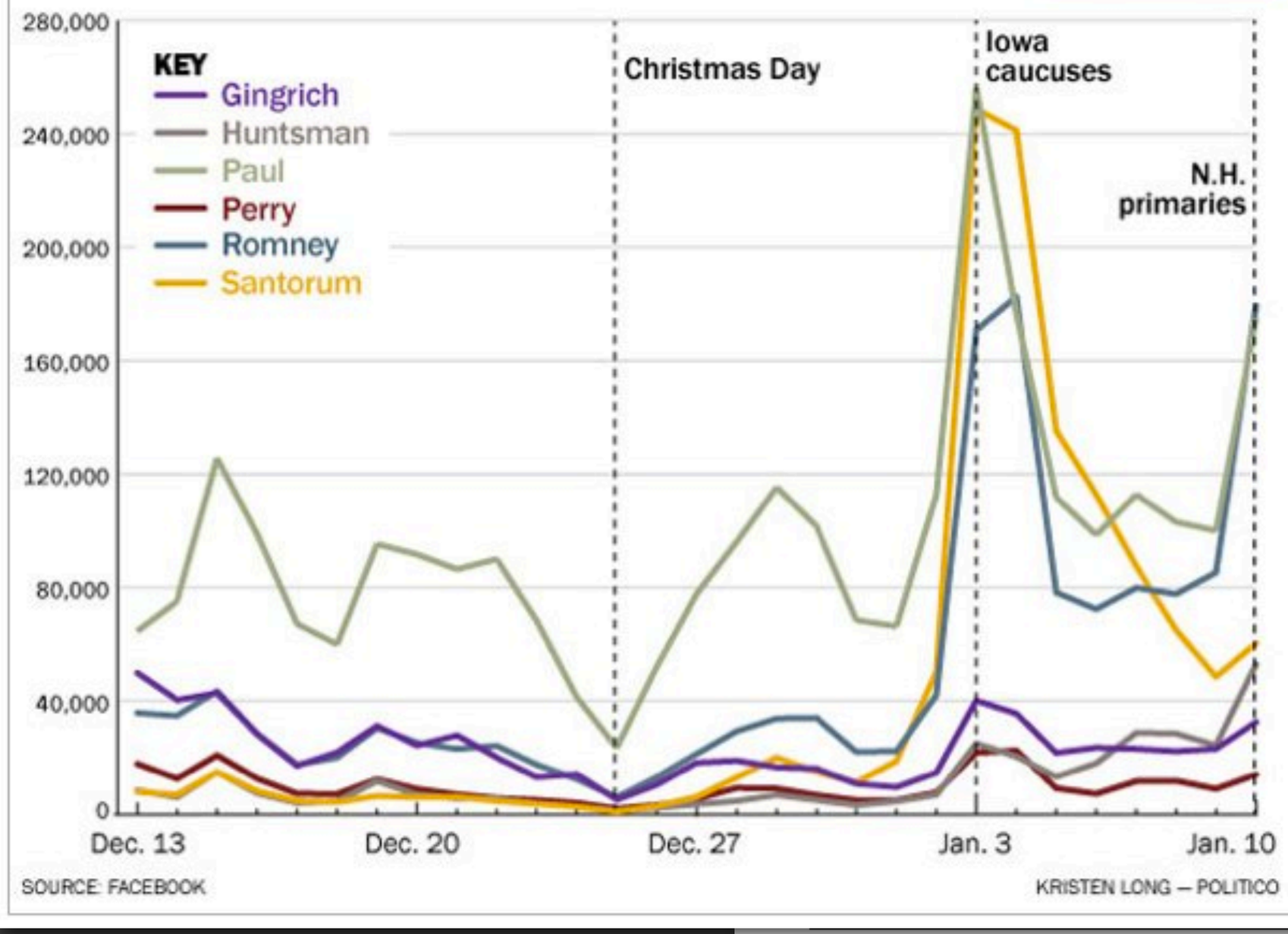
https://www.readwriteweb.com/archives/why_facebooks_data_sharing_matters.php

ReadWriteWeb

FACEBOOK MENTIONS BY CANDIDATE

Facebook measured the volume of its users' status updates, postings and comments over the last month to gauge the amount of social traffic around the Republican presidential contenders.

In partnership with facebook



SOURCE: FACEBOOK

KRISTEN LONG — POLITICO

https://www.readwriteweb.com/archives/why_facebooks_data_sharing_matters.php

ReadWriteWeb

Facebook has cut a deal with political website Politico that allows the independent site machine-access to Facebook users' messages, both public and private, when a Republican Presidential candidate is mentioned by name. The data is being collected and analyzed for sentiment by Facebook's data team, then delivered to Politico to serve as the basis of data-driven political analysis and journalism.

The move is being widely condemned in the press as a violation of privacy but if Facebook would do this right, it could be a huge win for everyone. Facebook could be the biggest, most dynamic census of human opinion and interaction in history. Unfortunately, failure to talk prominently about privacy protections, failure to make this opt-in (or even opt out!) and the inclusion of private messages are all things that put at risk any remaining shreds of trust in Facebook that could have served as the foundation of a new era of social self-awareness.

POLITICO

https://www.readwriteweb.com/archives/why_facebooks_data_sharing_matters.php

facebook

Ads help keep Facebook free

From the beginning, the people who built Facebook wanted it to be free for everyone. It now costs over a billion dollars a year to run Facebook, and delivering ads is how Facebook pays for this.

You can choose the ads you see

Unlike ads on television, you can impact the ads you see on Facebook. Spot something that doesn't interest you? Click the X and it's gone.

Like Send 70,029 people like this. Be the first of your friends.

https://www.facebook.com/about/ads

BETABEAT

Leaked Details of How Facebook Plans To Sell Your Timeline to Advertisers

What most users don't know is that the new features being introduced are all centered around increasing the value of Facebook to advertisers, to the point where Facebook representatives have been selling the idea that Timeline is actually about re-conceptualizing users around their consumer preferences, or as they put it, "brands are now an essential part of people's identities."

Disguising ads as your friends' updates is being offered up as an antidote to the dismal click-through rates for traditional web advertising. Sponsored stories in your feed and sidebar ads based on your friends' likes will become ubiquitous. Indeed in marketing materials, Facebook says these new premium ads are 90 percent accurate, compared to the industry average of 35 percent. "When people hear about you [the brand] from friends, they listen."

http://www.betabeat.com/2011/12/23/exclusive-leaked-details-of-how-facebook-plans-to-sell-your-timeline-to-advertisers

k Plans To
rs

Brands are now an essential part of people's identity

Disguising ads as your friends' upd
through rates for traditional web a
based on your friends' likes will beco
these new premium ads are 90 perce
"When people hear about you [the br

Custom Open Graph= Deeper connections to your brands

http://www.betabeat.com/2011/12/23/exclusive-leaked-details-of-how-facebook-plans-to-sell-your-timeline-to-advertisers

BETABEAT

Leaked Details of How Facebook Plans To Sell Your Timeline to Advertisers

What most users don't know is that the new features being introduced are all centered around increasing the value of Facebook to advertisers, to the point where Facebook representatives have been selling the idea that Timeline is actually about re-conceptualizing users around their consumer preferences, or as they put it, "brands are now an essential part of people's identities."

Disguising ads as your friends' updates is being offered up as an antidote to the dismal click-through rates for traditional web advertising. Sponsored stories in your feed and sidebar ads based on your friends' likes will become ubiquitous. Indeed in marketing materials, Facebook says these new premium ads are 90 percent accurate, compared to the industry average of 35 percent. "When people hear about you [the brand] from friends, they listen."

http://www.betabeat.com/2011/12/23/exclusive-leaked-details-of-how-facebook-plans-to-sell-your-timeline-to-advertisers

TIMELINE IS MANDATORY FOR ALL FACEBOOK USERS

TIMELINE IS MANDATORY FOR ALL FACEBOOK USERS WITH NO OPT-OUT OPTION

Facebook settles privacy case with the Federal Trade Commission

http://business.financialpost.com/2011/11/29/facebook-settles-privacy-case-wtih-ftc

Facebook has agreed to settle an investigation by the Federal Trade Commission into deceptive privacy practices, committing to cease making false claims and to submit to independent audits for 20 years.

The FTC said the world's largest Internet social network had been repeatedly deceptive. For example, Facebook promised users that it would not share personal information with advertisers, but it did, the agency said.

Also, the company failed to warn users that it was changing its website in December 2009 so that certain information that users designated as private, such as their "Friends List," would be made public, the FTC said.

"Facebook's innovation does not have to come at the expense of consumer privacy," FTC Chairman Jon Leibowitz said in a statement.

Facebook settles privacy case with the Federal Trade Commission

http://business.financialpost.com/2011/11/29/facebook-settles-privacy-case-wtih-ftc

Facebook settles privacy case with the Federal Trade Commission

Facebook has agreed to settle an investigation by the Federal Trade Commission into deceptive privacy practices, committing to cease making false claims and to submit to independent audits for 20 years.

The FTC said the world's largest Internet social network had been repeatedly deceptive. For example Facebook promised users that it would not share personal information with advertisers, but it did, the agency said.

Also, the company failed to warn users that it was changing its website in December 2009 so that certain information that users designated as private, such as their "Friends List," would be made public, the FTC said.

"Facebook's innovation does not have to come at the expense of consumer privacy," FTC Chairman Jon Leibowitz said in a statement.

http://business.financialpost.com/2011/11/29/facebook-settles-privacy-case-wtih-ftc

Facebook's business model came under fire in the EU

http://venturebeat.com/2011/11/28/facebook-advertising-eu

Facebook's business model is under fire in the EU

The EU is considering a ban on Facebook's practice of selling demographic data to marketers and advertisers without specific permission from users.

Now, however, the EC is planning to ban such activity unless users themselves specifically agree to it. The EU's data protection working group is currently investigating how Facebook tracks users, stores data and uses that information to serve targeted ads.

The European Commission is planning to stop the way the website "eavesdrops" on its users to gather information about their political opinions, sexuality, religious beliefs – and even their whereabouts.

Viviane Reding, the vice president of European Commission, said the Directive would amend current European data protection laws in the light of technological advances and ensure consistency in how offending firms are dealt with across the EU.

http://venturebeat.com/2011/11/28/facebook-advertising-eu

http://www.telegraph.co.uk/technology/facebook/8917836/Facebook-faces-EU-curbs-on-selling-users-interests-to-advertisers.html

Facebook's entire business model is under fire in the EU

The EU is considering a ban on Facebook's practice of selling demographic data to marketers and advertisers without specific permission from users.

Now, however, the EC is planning to ban such activity unless users themselves specifically agree to it. The EU's data protection working group is currently investigating how Facebook tracks users, stores data and uses that information to serve targeted ads.

[...] The European Commission is planning to stop the way the website "eavesdrops" on its users to gather information about their political opinions, sexuality, religious beliefs – and even their whereabouts.

Viviane Reding, the vice president of European Commission, said the Directive would amend current European data protection laws in the light of technological advances and ensure consistency in how offending firms are dealt with across the EU.

http://venturebeat.com/2011/11/28/facebook-advertising-eu

http://www.telegraph.co.uk/technology/facebook/8917836/Facebook-faces-EU-curbs-on-selling-users-interests-to-advertisers.html

Facebook threatened by German consumer group over App Center privacy info

http://www.zdnet.com/facebook-threatened-by-german-consumer-group-over-app-center-privacy-info-7000003309/

Facebook threatened by German consumer group over App Center privacy info

The problem, according to the consumer protection group, is in the "non-exhaustive" information that the App Center shows in small grey writing before the user chooses to click "play game", "send to mobile" or "visit website".

[The Verbraucherzentrale Bundesverband] VZBV said on Monday that Facebook was breaking European data protection law by not explicitly inviting the user to give their consent.

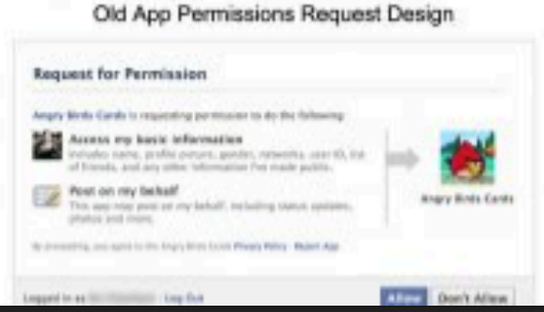
http://www.zdnet.com/facebook-threatened-by-german-consumer-group-over-app-center-privacy-info-7000003309/

5 Design Tricks Facebook Uses To Affect Your Privacy Decisions

AVI CHARKHAM

Saturday, August 25th, 2012 **91 Comments**

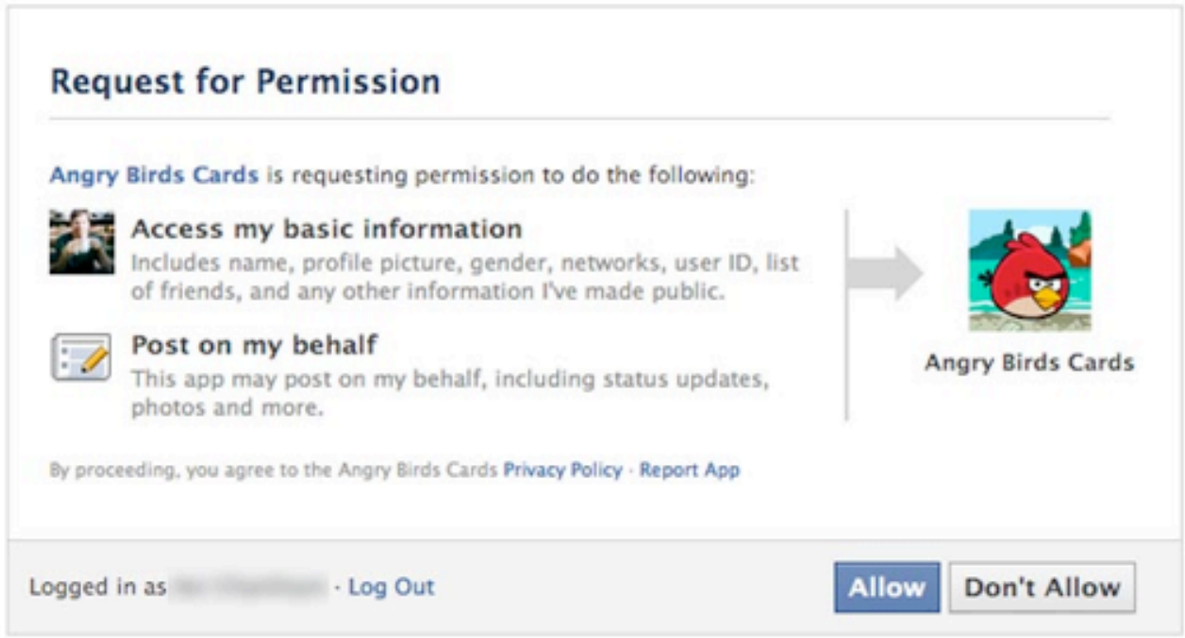
Old App Permissions Request Design



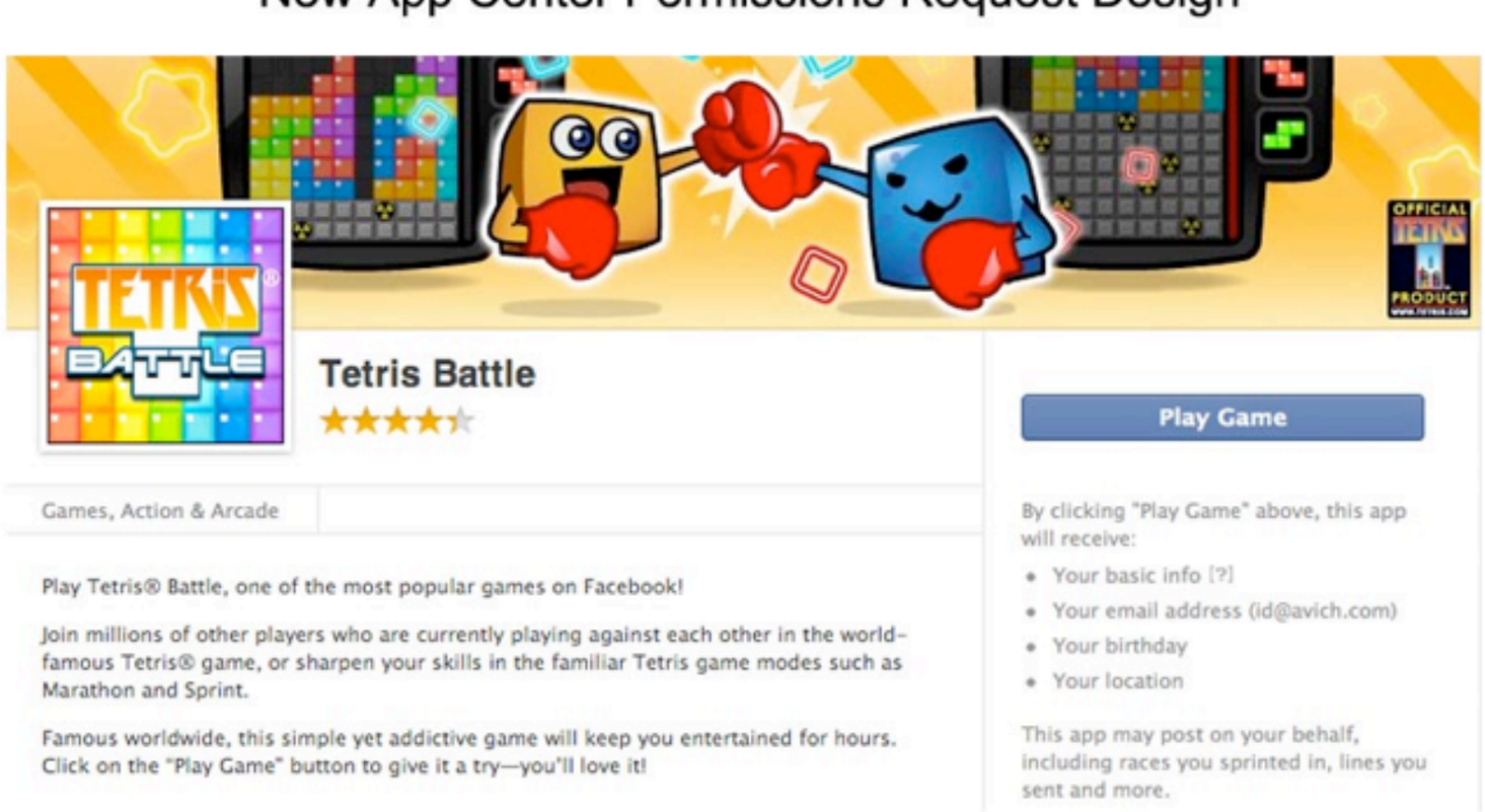
Editor's note: *Avi Charkham is Head of Product & Design @* ***lool ventures****, an early stage, value-add venture capital firm based in Israel and the incubators of* ***MyPermissions*** *personal cloud security service.*

http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/

Old App Permissions Request Design

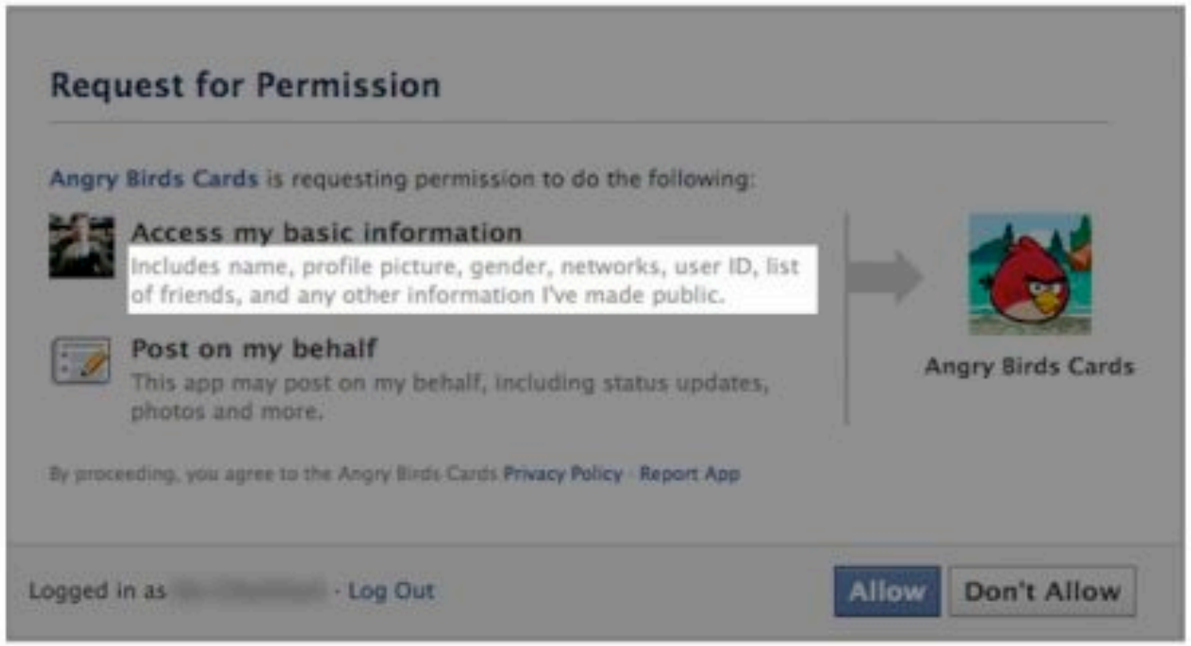


New App Center Permissions Request Design

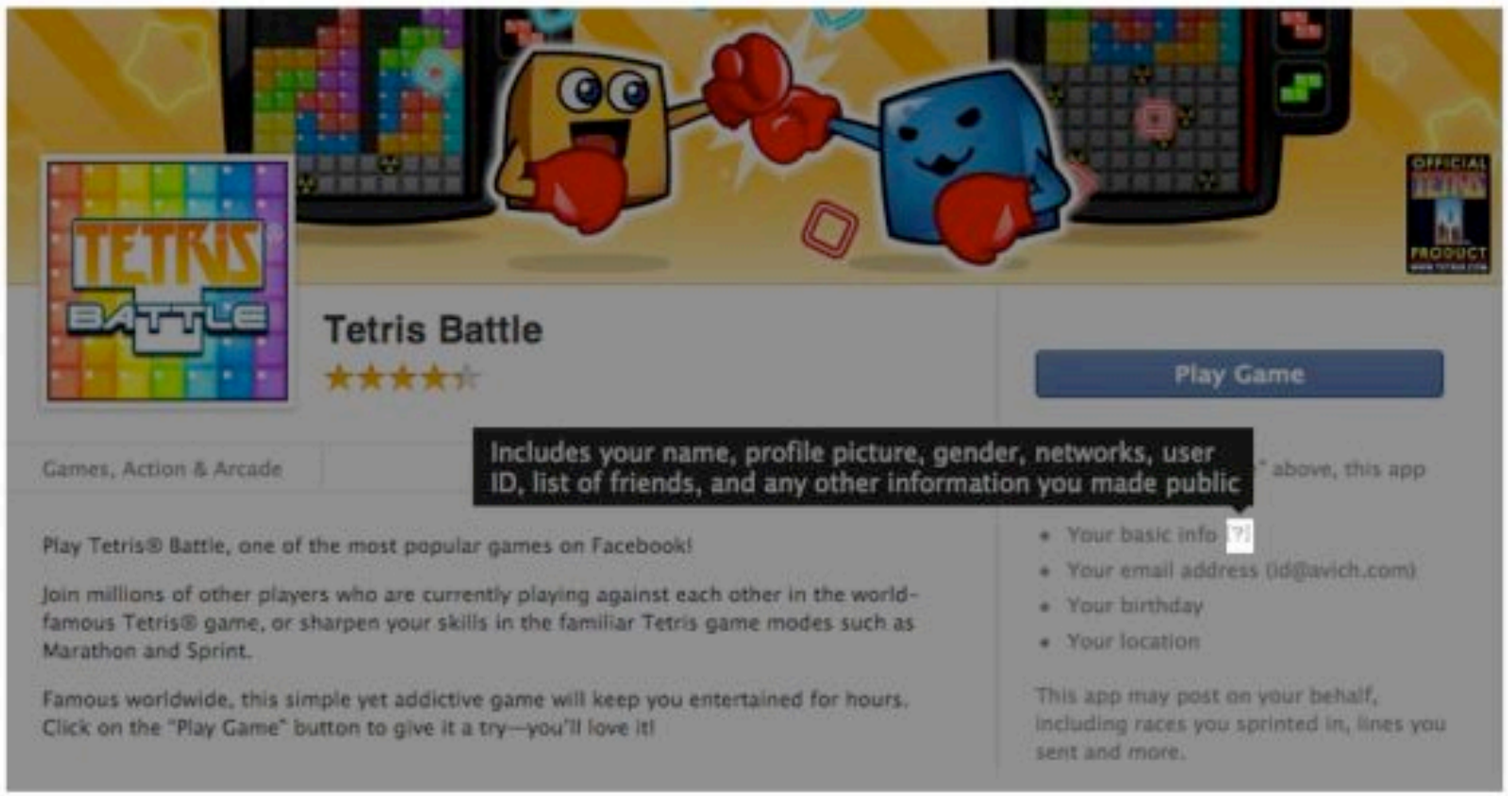


http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/

Old Design: **Detailed & Visible** Permissions

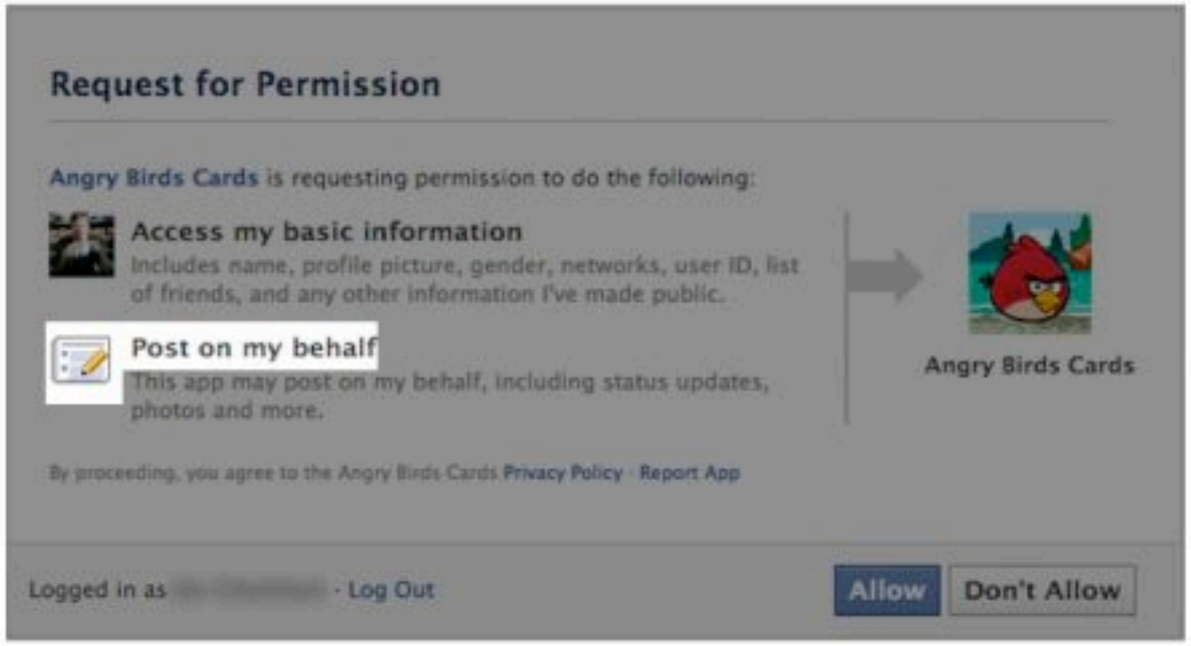


New Design: **Hidden** Permissions

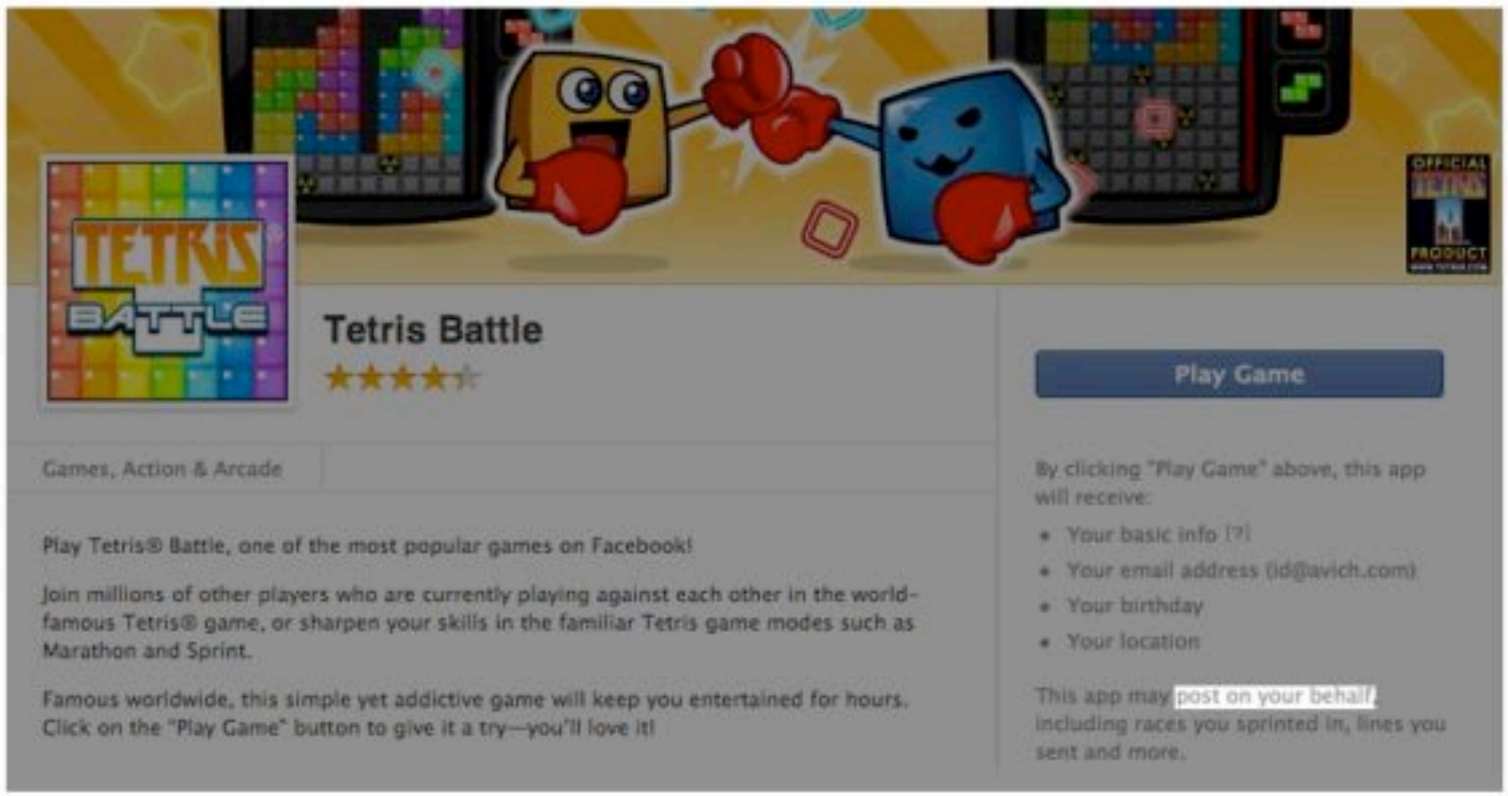


http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/

Old Design: **Bold Black Font** + Prominant Permission Icon

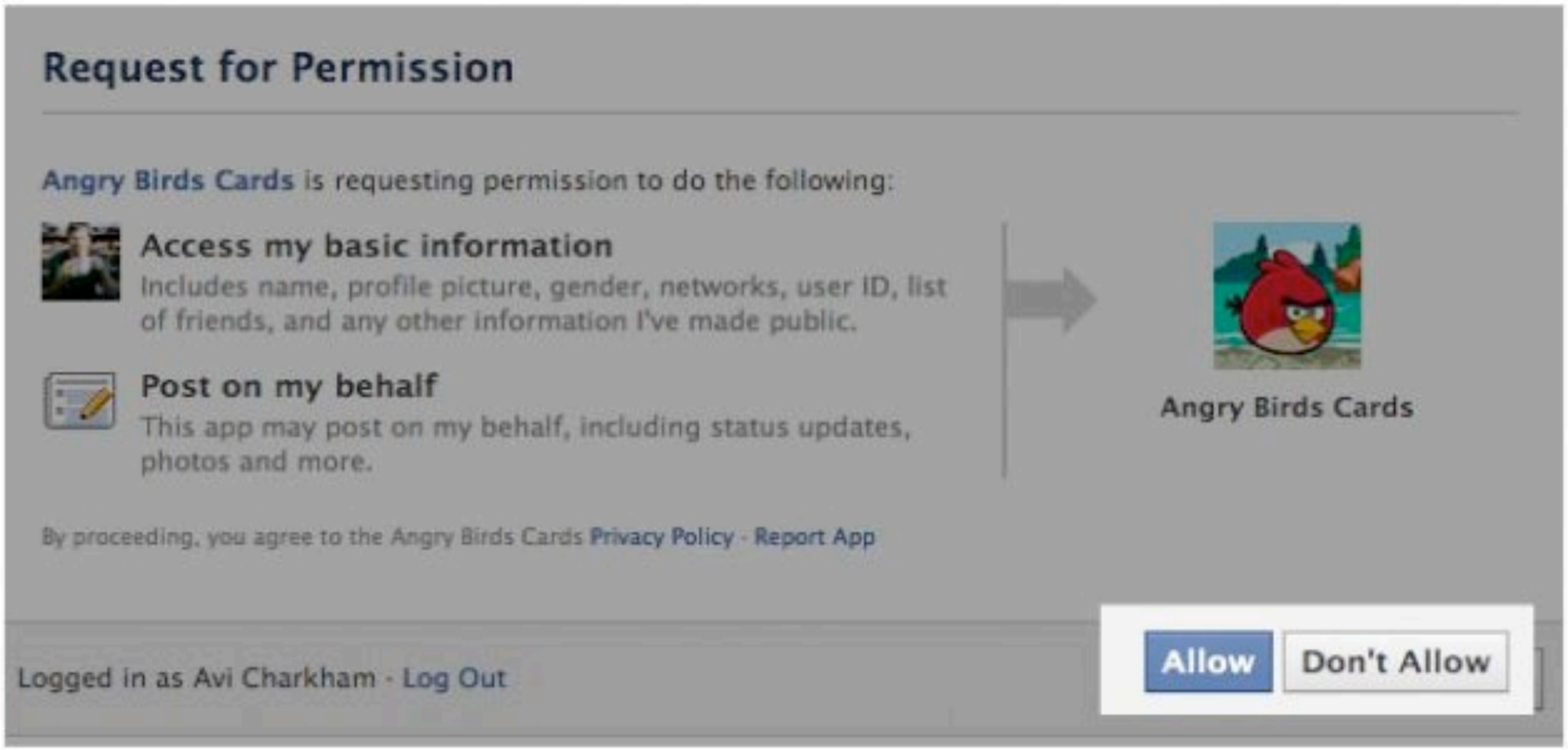


New Design: Tiny Gray Font

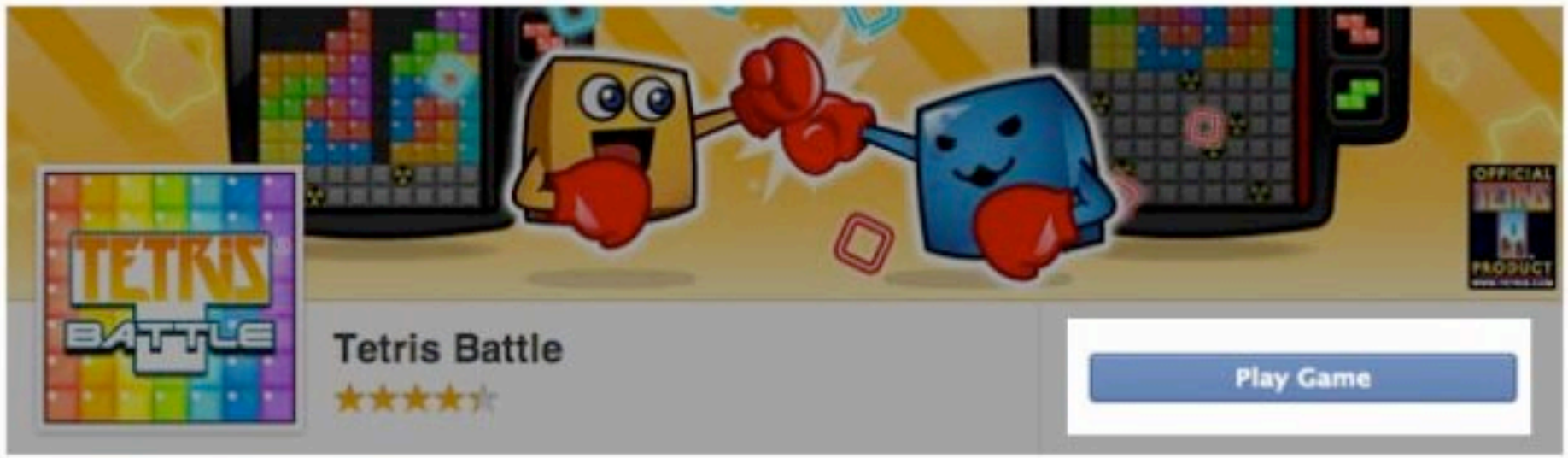


http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/

Old Design: 2 Buttons = **Choice**



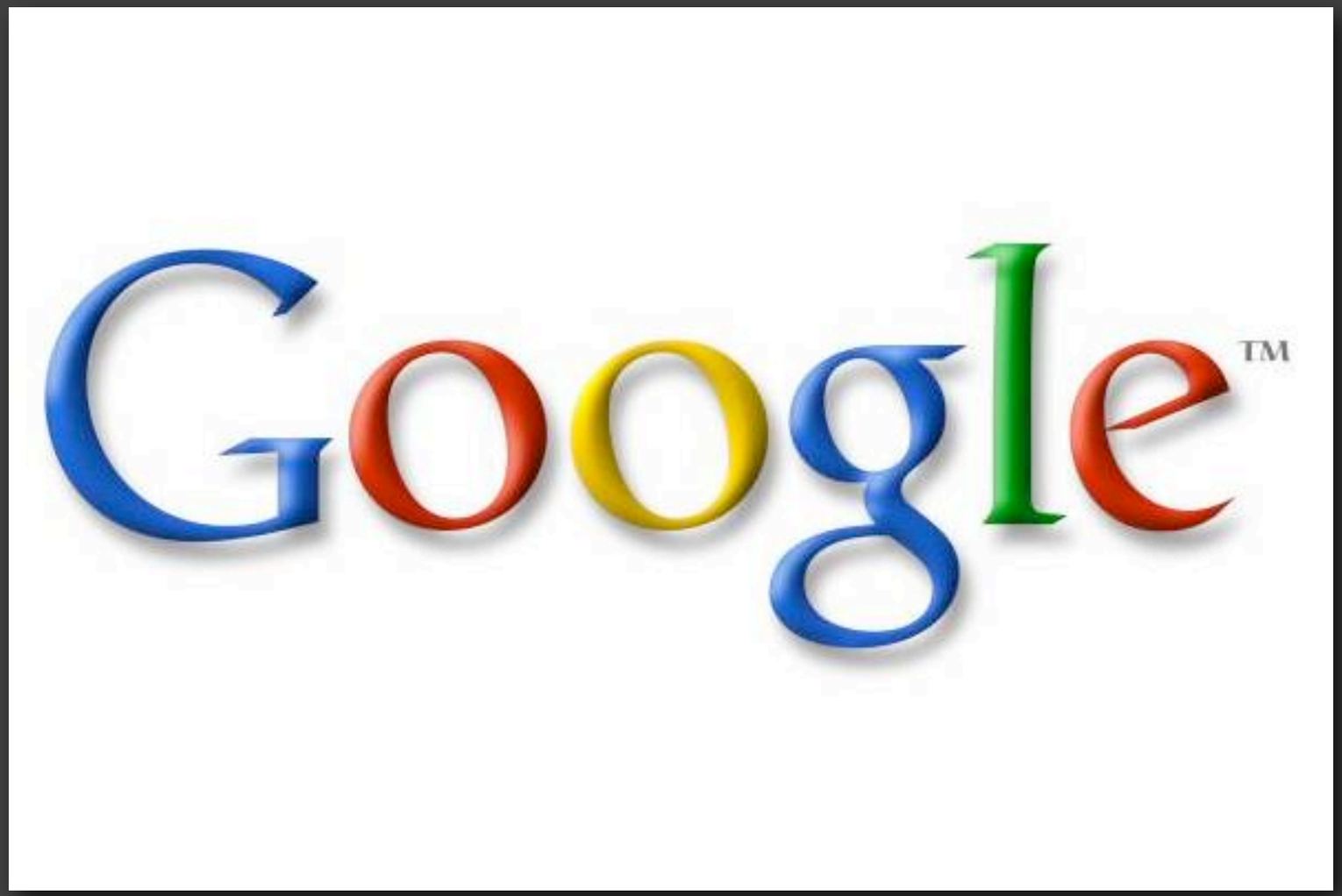
New Design: 1 Button = **No Choice**

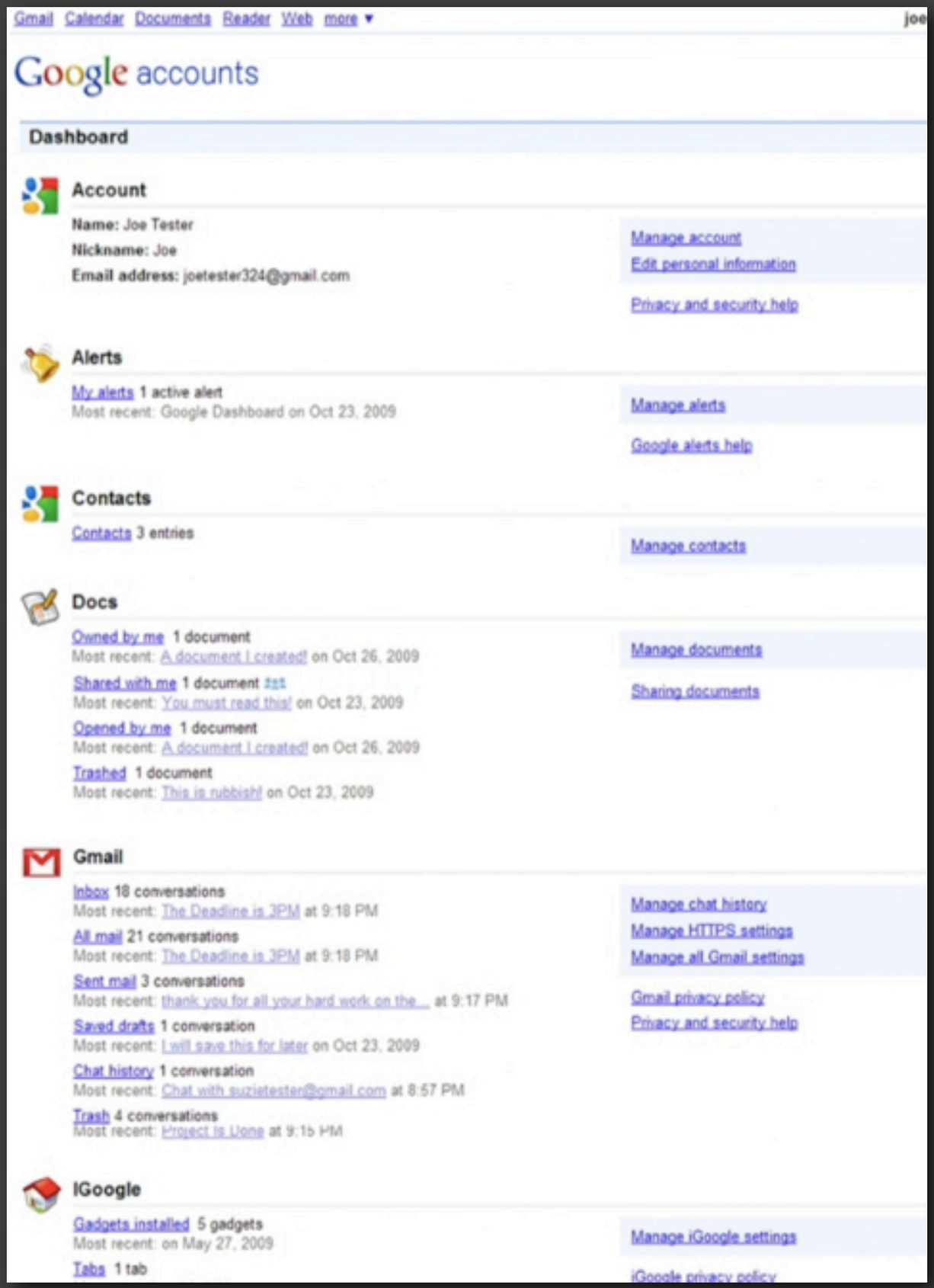


http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/

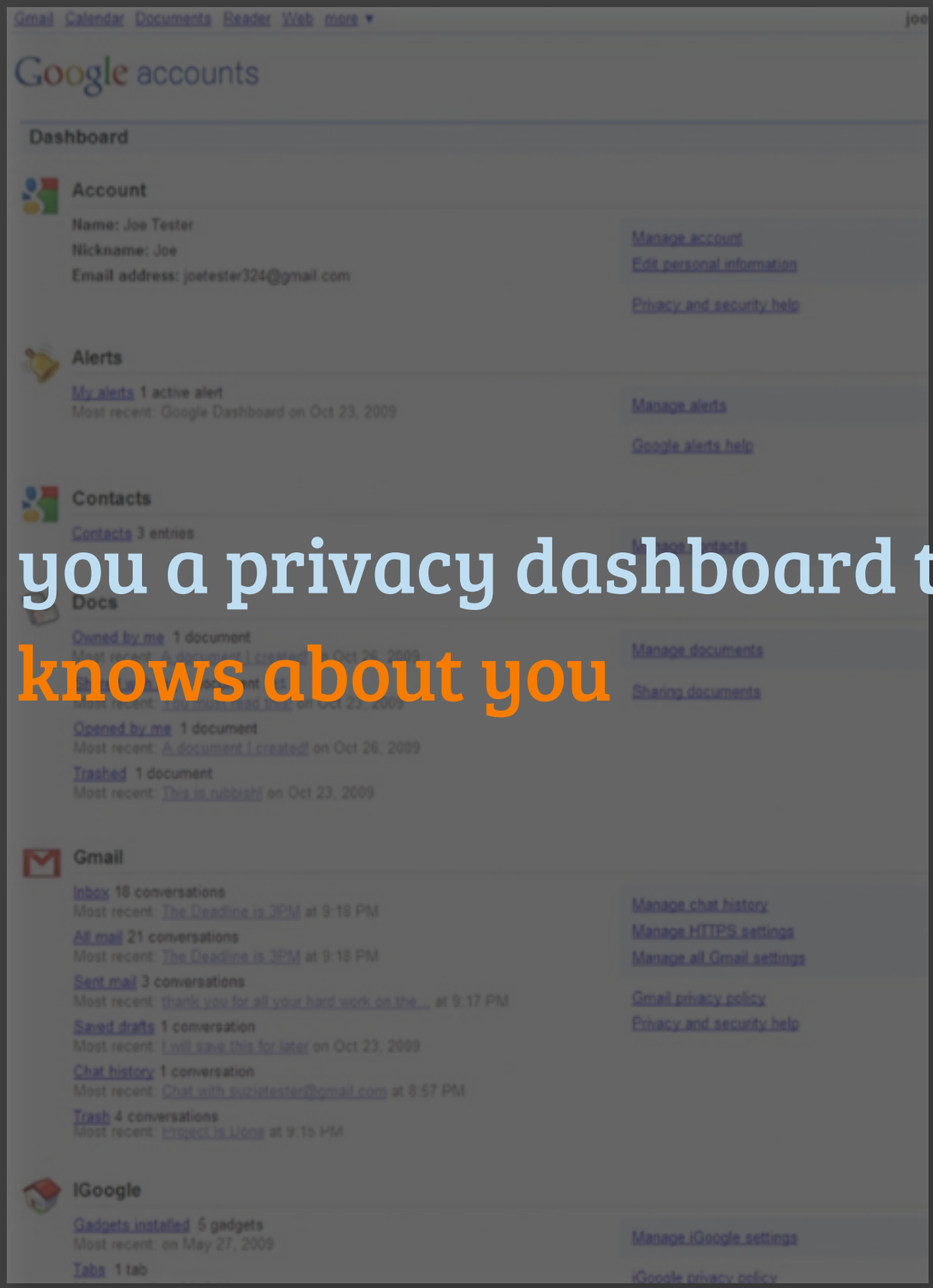
DESIGN CHOICES ARE INTENDED TO MAKE YOU PART WITH YOUR PERSONAL INFORMATION

http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/


Google™



http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you

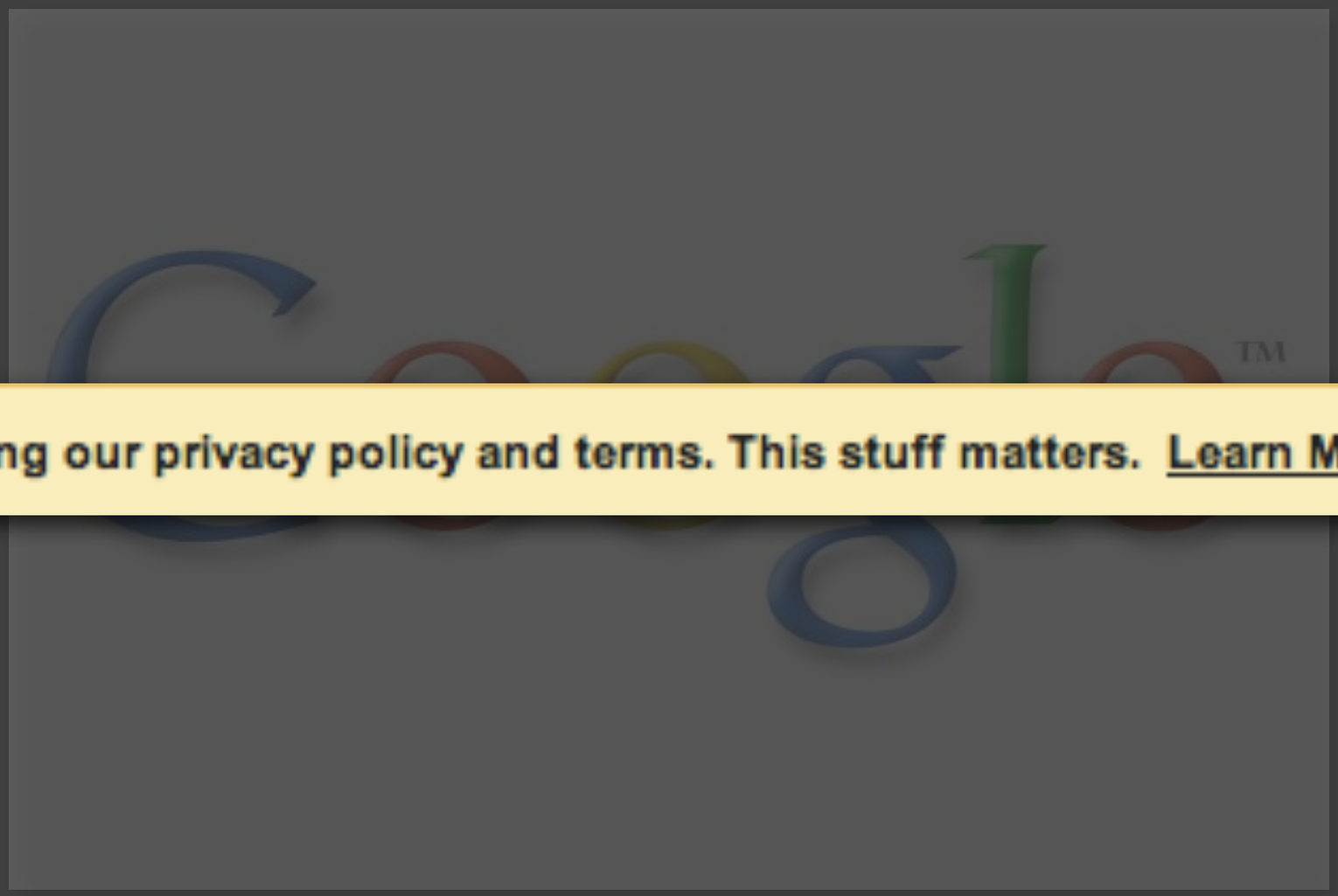


Google gives you a privacy dashboard to show just how much it knows about you

http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you

“Your profile is the way you present yourself on Google products and across the web. With your profile, you can manage the information that people see - such as your bio, contact details, and links to other sites about you or created by you.”

https://profiles.google.com



Google changes privacy across all products

"Google said [...] it will require users to allow the company to follow their activities across e-mail, search ... and other services, a radical shift in strategy that is expected to invite greater scrutiny of its privacy and competitive practices."

http://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html

Google's new policy replaces more than 60 existing product-specific privacy documents for services including Gmail, YouTube and Google Docs (plus Picassa, Blogger, Google Talk, Google Earth, etc.)

Google says the unified terms will provide better search results and serve up ads that are more likely to be of interest.

http://www.scientificamerican.com/article.cfm?id=how-googles-new-privacy-p

"...[Google] said it may combine the information users submit under their email accounts with information from other Google services or third parties. What people do and share on the social networking site Google+, Gmail and YouTube will be combined to create a more three-dimensional picture of consumers' likes and dislikes, according to reports. Google did not return calls seeking comment."

http://blogs.smartmoney.com/advice/2012/01/25/who-would-pay-5000-to-use-google-you

SCIENTIFIC AMERICAN™

"If Google received a warrant to disclose documents, and your business and personal docs are intermingled — that's a problem," he said. "Some would like to say, "No, thank you" and keep their accounts separate."

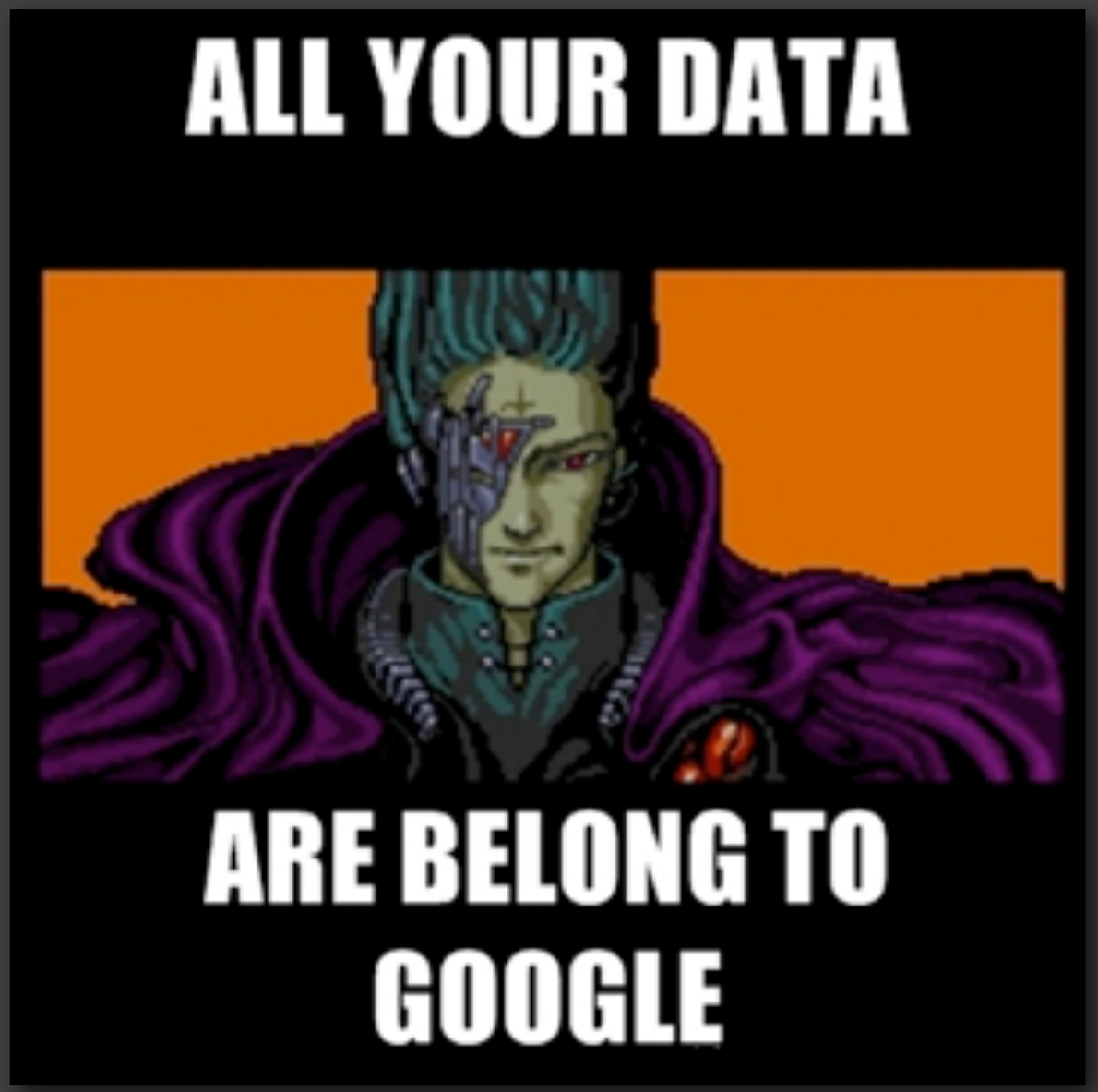
"Google should make it easy for people to set up and manage separate accounts if they wish to do so," Kurt Opsahl, senior staff attorney for the Electronic Frontier Foundation.

http://www.scientificamerican.com/article.cfm?id=how-googles-new-privacy-p

The End of Privacy?

If Google can change its privacy policy today, it can change it tomorrow. And it will. [...] This is what's motivating their policy change this week, and someday it's likely to motivate them to sell my personal information after all.

http://www.flickr.com/photos/47691521@N07/4638981545
http://motherjones.com/kevin-drum/2012/01/end-privacy-google



https://en.wikipedia.org/wiki/All_your_base_are_belong_to_us

GOOGLE CHANGES PRIVACY POLICY ACROSS ALL PRODUCTS

GOOGLE CHANGES PRIVACY POLICY ACROSS ALL PRODUCTS WITH NO OPT-OUT OPTION

FEDERAL TRADE COMMISSION

Protecting America's Consumers

Privacy Policy | Cor

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions | C

About Public Affairs | Public Events | Speeches | Webcasts | Reporter Resources | Noticias en

For Release: 03/30/2011

FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network

Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data

Google Inc. has agreed to settle Federal Trade Commission charges that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. The agency alleges the practices violate the FTC Act. The proposed settlement bars the company from future privacy misrepresentations, requires it to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years. This is the first time an FTC settlement order has required a company to implement a comprehensive privacy program to protect the privacy of consumers' information. In addition, this is the first time the FTC has alleged violations of the substantive privacy requirements of the U.S.-EU Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data lawfully from the European Union to the United States.

http://www.ftc.gov/opa/2011/03/google.shtm

On the day Buzz was launched, Gmail users got a message announcing the new service and were given two options: “Sweet! Check out Buzz,” and “Nah, go to my inbox.” However, the FTC complaint alleged that some Gmail users who clicked on “Nah…” were nonetheless enrolled in certain features of the Google Buzz social network.

For those Gmail users who clicked on “Sweet!,” the FTC alleges that they were not adequately informed that the identity of individuals they emailed most frequently would be made public by default. Google also offered a “Turn Off Buzz” option that did not fully remove the user from the social network.

http://www.ftc.gov/opa/2011/03/google.shtm

On the day Buzz was launched, Gmail users got a message announcing the new service and were given two options: "Sweet! Check out Buzz," and "Nah, go to my inbox." However, the FTC complaint alleged that some Gmail users who clicked on "Nah..." were nonetheless enrolled in certain features of the Google Buzz social network.

For those Gmail users who clicked on "Sweet!," the FTC alleges that they were not adequately informed that the identity of individuals they emailed most frequently would be made public by default. Google also offered a "Turn Off Buzz" option that did not fully remove the user from the social network.

http://www.ftc.gov/opa/2011/03/google.shtm

In response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors. According to the FTC complaint, Google made certain changes to the Buzz product in response to those complaints.

When Google launched Buzz, its privacy policy stated that "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use." The FTC complaint charges that Google violated its privacy policies by using information provided for Gmail for another purpose - social networking - without obtaining consumers' permission in advance.

http://www.ftc.gov/opa/2011/03/google.shtm

In response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors. According to the FTC complaint, Google made certain changes to the Buzz product in response to those complaints.

When Google launched Buzz, its privacy policy stated that "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use." The FTC complaint charges that Google violated its privacy policies by using information provided for Gmail for another purpose - social networking - without obtaining consumers' permission in advance.

http://www.ftc.gov/opa/2011/03/google.shtm

https://plus.google.com

Identity Matters

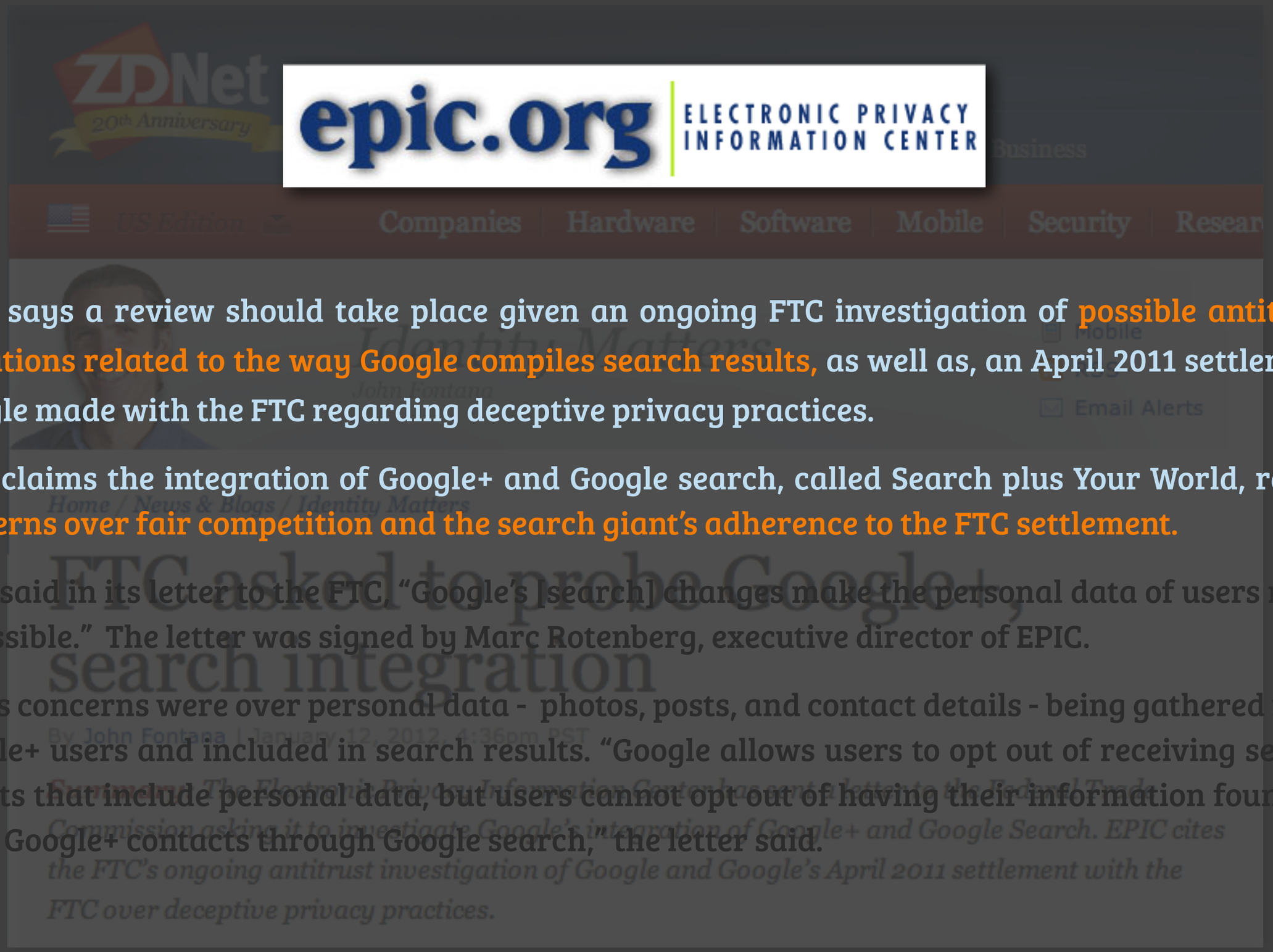
John Fontana

FTC asked to probe Google+, search integration

By John Fontana | January 12, 2012, 4:36pm PST

Summary: *The Electronic Privacy Information Center has sent a letter to the Federal Trade Commission asking it to investigate Google's integration of Google+ and Google Search. EPIC cites the FTC's ongoing antitrust investigation of Google and Google's April 2011 settlement with the FTC over deceptive privacy practices.*

http://www.zdnet.com/blog/identity/ftc-asked-to-probe-google-search-integration/143

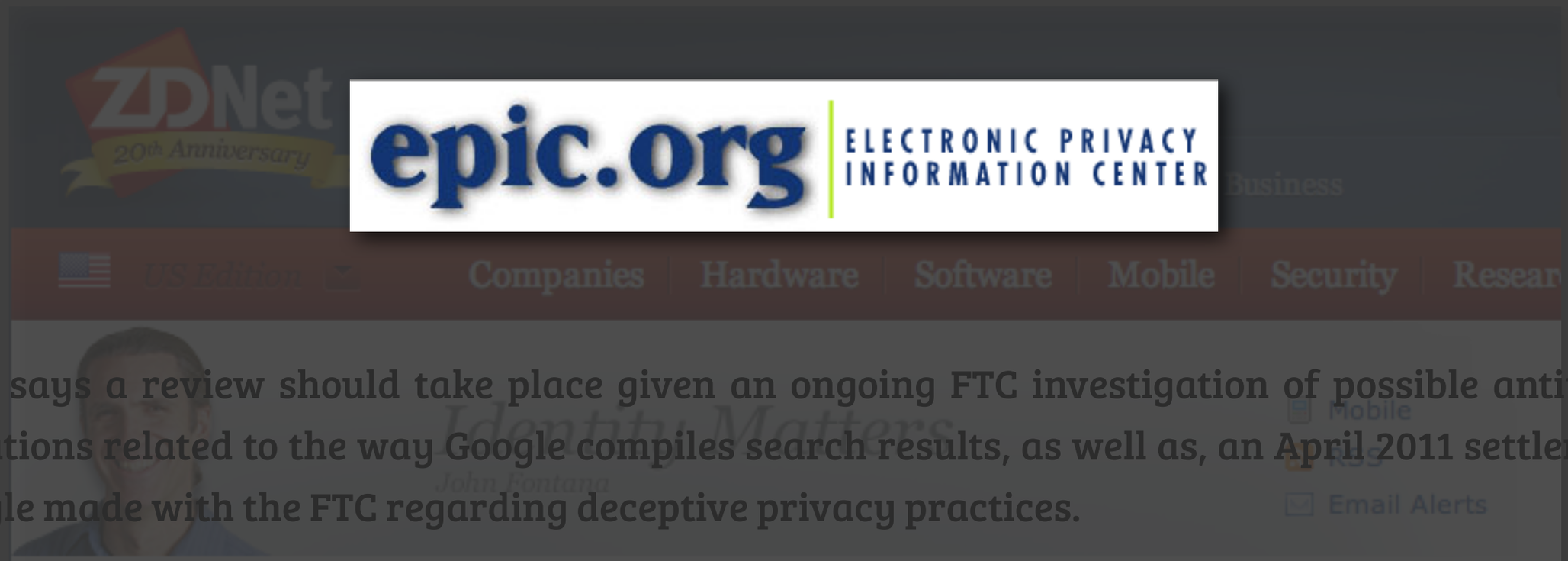


EPIC says a review should take place given an ongoing FTC investigation of possible antitrust violations related to the way Google compiles search results, as well as, an April 2011 settlement Google made with the FTC regarding deceptive privacy practices.

EPIC claims the integration of Google+ and Google search, called Search plus Your World, raises concerns over fair competition and the search giant's adherence to the FTC settlement.

EPIC said in its letter to the FTC, "Google's [search] changes make the personal data of users more accessible." The letter was signed by Marc Rotenberg, executive director of EPIC.

EPIC's concerns were over personal data - photos, posts, and contact details - being gathered from Google+ users and included in search results. "Google allows users to opt out of receiving search results that include personal data, but users cannot opt out of having their information found by their Google+ contacts through Google search," the letter said.



EPIC says a review should take place given an ongoing FTC investigation of possible antitrust violations related to the way Google compiles search results, as well as, an April 2011 settlement Google made with the FTC regarding deceptive privacy practices.

EPIC claims the integration of Google+ and Google search, called Search plus Your World, raises concerns over fair competition and the search giant's adherence to the FTC settlement.

EPIC said in its letter to the FTC, "Google's [search] changes make the personal data of users more accessible." The letter was signed by Marc Rotenberg, executive director of EPIC.

EPIC's concerns were over personal data - photos, posts, and contact details - being gathered from Google+ users and included in search results. "Google allows users to opt out of receiving search results that include personal data, but users cannot opt out of having their information found by their Google+ contacts through Google search," the letter said.

http://www.zdnet.com/blog/identity/ftc-asked-to-probe-google-search-integration/143

Search Plus is combining personal signals — your search and web history — along with social signals to create a new form of personalized results. It's not just who you are that now influences what you see. It's who you know. What your friends like, share or create can influence what shows up first when you search for something.

http://marketingland.com/faq-google-search-plus-your-world-3533

Google may use your Google account information, such as items you +1 on Google properties and across the web, to personalize content and ads on non-Google websites.

http://www.google.com/privacy/ads

Google Under Fire for Circumvention of Cookie Settings in Safari for iOS to Track Users

http://www.macrumors.com/2012/02/17/google-under-fire-for-circumvention-of-cookie-settings-in-safari-for-ios-to-track-users

Safari's cookie blocking feature is unique in two ways: its default and its substantive policy.

Unlike every other browser vendor, Apple enables 3rd party cookie blocking by default. Every iPhone, iPad, iPod Touch, and Mac ships with the privacy feature turned on.

Apple's Safari web browser is configured to block third-party cookies by default. We identified four advertising companies that unexpectedly place trackable cookies in Safari. Google and Vibrant Media intentionally circumvent Safari's privacy feature. Media Innovation Group and PointRoll serve scripts that appear to be derived from circumvention example code.

http://webpolicy.org/2012/02/17/safari-trackers

Safari's cookie blocking feature is unique in two ways: its default and its substantive policy.

Unlike every other browser vendor, Apple enables 3rd party cookie blocking by default. Every iPhone, iPad, iPod Touch, and Mac ships with the privacy feature turned on.

Apple's Safari web browser is configured to block third-party cookies by default. We identified four advertising companies that unexpectedly place trackable cookies in Safari. Google and Vibrant Media intentionally circumvent Safari's privacy feature. Media Innovation Group and PointRoll serve scripts that appear to be derived from circumvention example code.

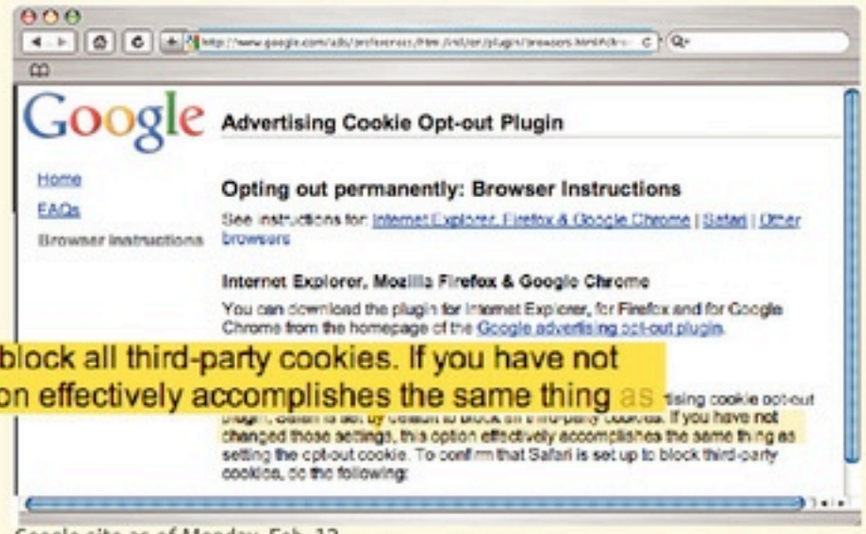
http://webpolicy.org/2012/02/17/safari-trackers

Google's Technique: How It Worked

The Internet giant circumvented privacy settings on Apple's Safari browser.

Safari automatically prevents installation of 'cookies'—small files that can track a person's Web browsing—from ad networks and other so-called third parties.

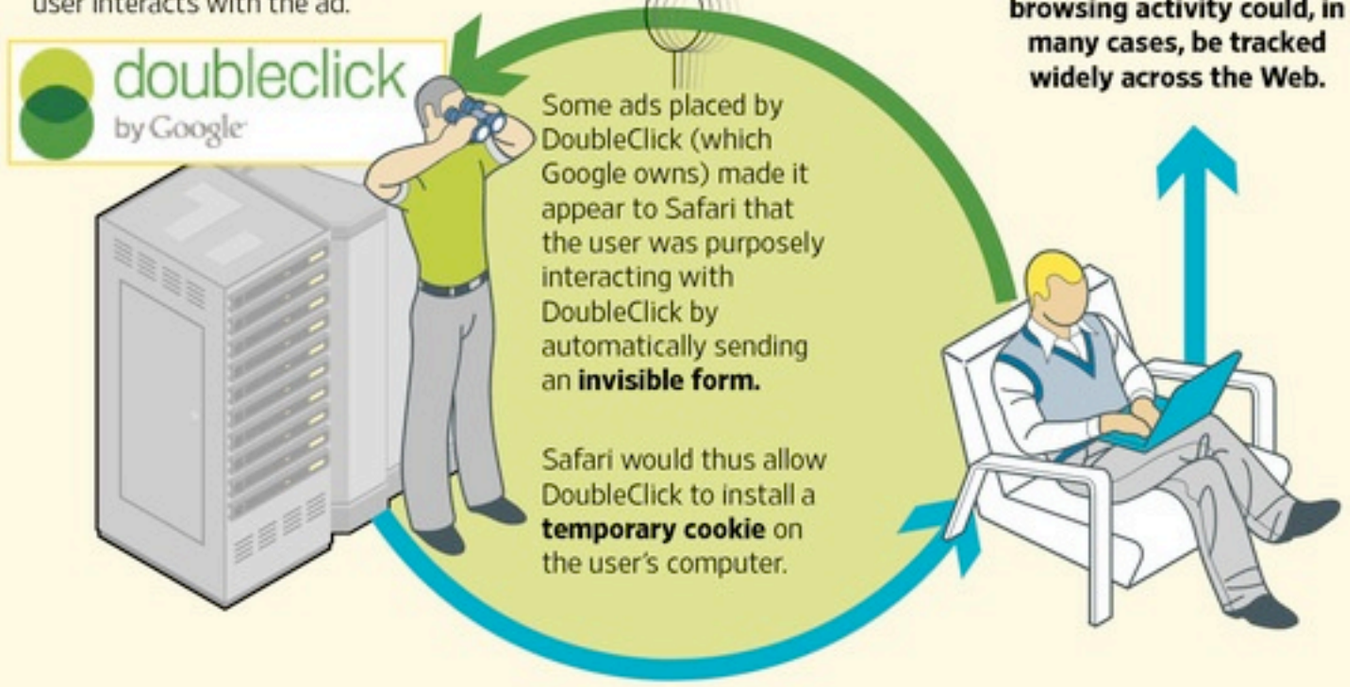
Google until recently assured Safari users on one of its sites that, because of this, they don't need to opt out of Google tracking:



plugin, **Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as** setting the opt-out cookie. To confirm that Safari is set up to block third-party cookies, do the following:

Google site as of Monday, Feb. 12

However, Google exploited a **loophole** in Safari: it allows an advertiser to place a cookie if the user interacts with the ad.



http://webpolicy.org/2012/02/17/safari-trackers

http://www.macrumors.com/2012/02/17/google-under-fire-for-circumvention-of-cookie-settings-in-safari-for-ios-to-track-users

- Google used a loophole to make Safari allow cookies (which it will only do IF a user interacts with an ad)
- an ad from DoubleClick (owned by Google) sent an invisible form, so Safari would think the user was interacting with the ad
- thus, cookie accepted, tracking occurred
- Google discouraged Safari users to opt-out

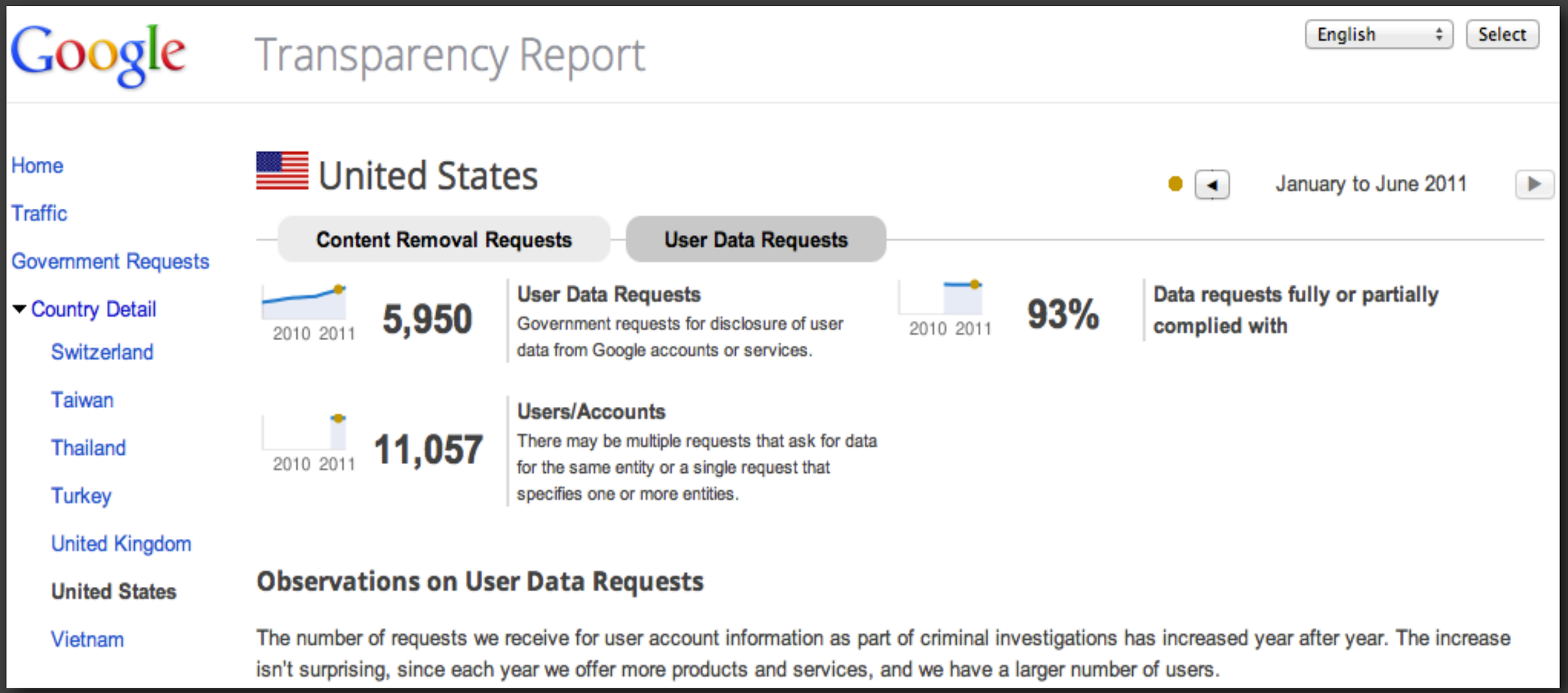
http://webpolicy.org/2012/02/17/safari-trackers
http://www.macrumors.com/2012/02/17/google-under-fire-for-circumvention-of-cookie-settings-in-safari-for-ios-to-track-users

Google settles Safari suit for $22.5 million

https://www.competitionpolicyinternational.com/google-to-settle-safari-suit-for-22-5-million/

GOOGLE PUBLICIZED USER'S PRIVATE DATA AND ALSO WORKED AROUND BROWSER SECURITY SETTINGS

Lastly, Google produces a laudable transparency report, but...



"Google complies with 93 percent of the 6,000 requests it receives for user data from law enforcement agencies is very different from the approach news organizations would take to handing over sources."

https://www.google.com/transparencyreport/governmentrequests/US/?p=2011-06&t=USER_DATA_REQUEST

http://allthingsd.com/20130611/google-wants-permission-to-disclose-how-many-national-security-requests-it-gets/

Google Wants Permission to Disclose How Many National Security Requests It Gets

"We therefore ask you to help make it possible for Google to publish in our Transparency Report aggregate numbers of national security requests, including FISA disclosures—in terms of both the number we receive and their scope. Google's numbers would clearly show that our compliance with these requests falls far short of the claims being made. Google has nothing to hide"

http://allthingsd.com/20130611/google-wants-permission-to-disclose-how-many-national-security-requests-it-gets/

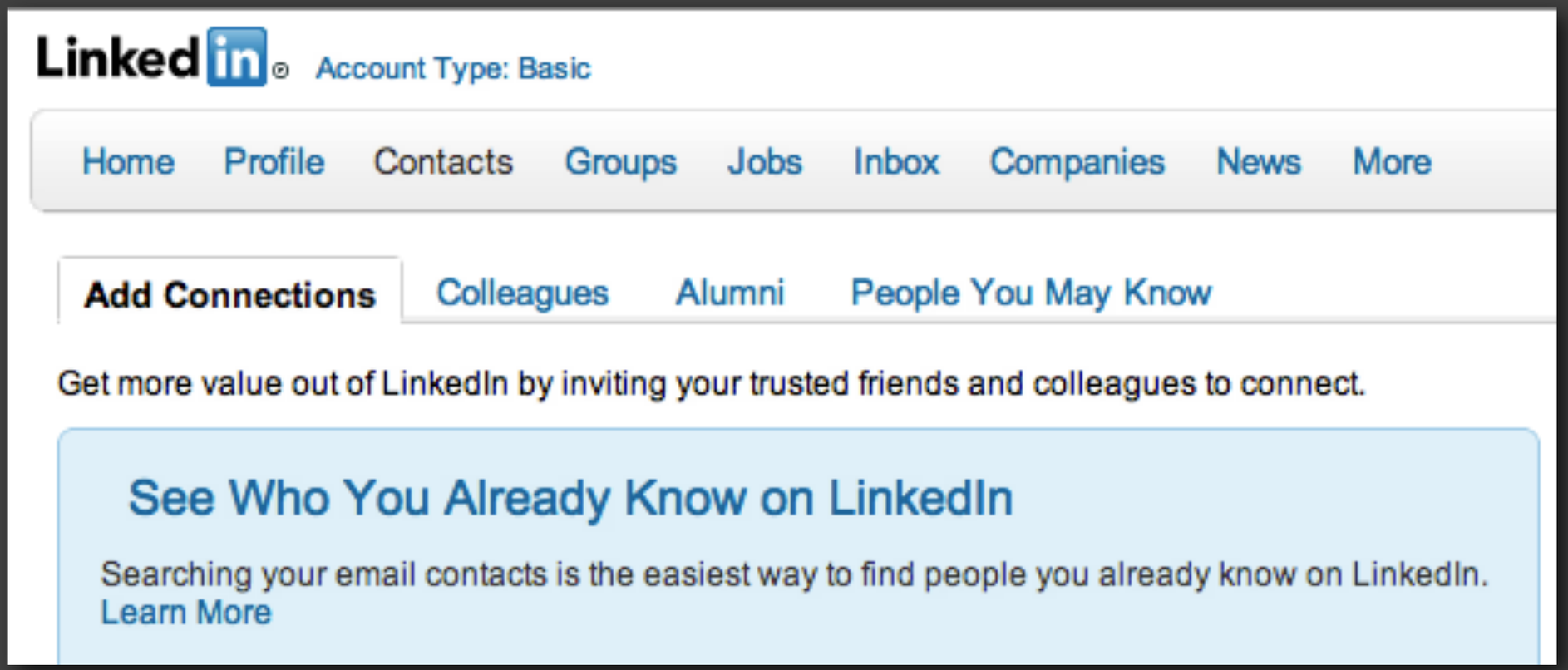
Google challenges U.S. gag order, citing First Amendment

"Google asked the secretive Foreign Intelligence Surveillance Court on Tuesday to ease long-standing gag orders over data requests the court makes, arguing that the company has a constitutional right to speak about information it is forced to give the government. [...] A high-profile legal showdown might help Google's efforts to portray itself as aggressively resisting government surveillance, and a victory could bolster the company's campaign to portray government surveillance requests as targeted narrowly and affecting only a small number of users"

http://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html

"...all these concerns about privacy tend to be old people issues." Reid Hoffman, the founder of LinkedIn, in a segment during last year's World Economic Forum at Davos, Switzerland

http://www.businessinsider.com/privacy-is-for-old-people-says-linkedin-founder-2011-10



http://www.businessinsider.com/privacy-is-for-old-people-says-linkedin-founder-2011-10

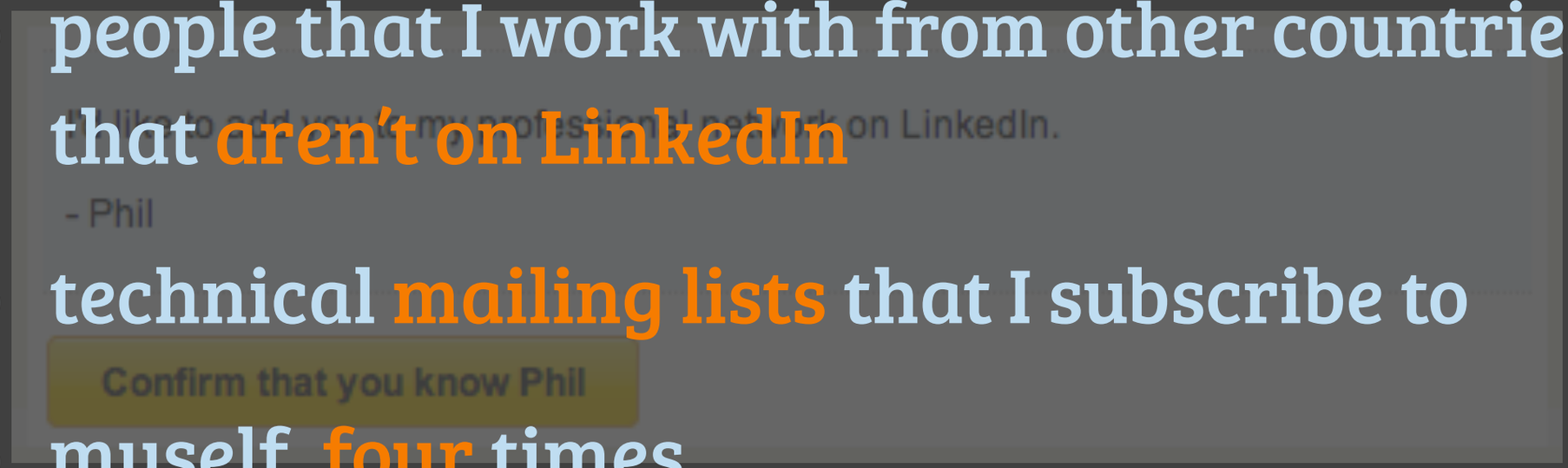
I'd like to add you to my professional network on LinkedIn.

- Phil

Confirm that you know Phil

http://fak3r.com/2011/10/12/linkedin-is-spamming-all-of-my-gmail-contacts

- people I didn't know well personally
- people that I work with from other countries that aren't on LinkedIn



- technical mailing lists that I subscribe to
- myself, four times
- and in one case, a deceased relative

http://fak3r.com/2011/10/12/linkedin-is-spamming-all-of-my-gmail-contacts

« HOWTO install php5-fpm on Debian Squeeze

HOWTO run DD-WRT on a Netgear WNDR3700 »

LinkedIn is spamming all of my Gmail contacts

UPDATE2 I finally got a response on Thu, Oct 27, 2011 at 7:24 AM, it said, "*I would first like to apologize for the delay in responding to your inquiry. This is certainly not the customary wait time for a reply from LinkedIn Customer Support. We have been experiencing higher than expected volumes, and your patience is greatly appreciated.*" So, they've been so busy that it took 2 1/2 weeks to get back to me? Still, they haven't answered my questions, one what happened and two, who did they email on my behalf? I need a list. Stay tuned.

Linkedin...good idea, bad idea?

UPDATE today is October 17, 2011, so it's been a week since I've reported my problem, and I have not gotten anything back from LinkedIn support. Pathetic.

FAK3R

look lout honey, cause I'm using technology

Search

Move along nothing to see here

Here are some recommended categories of mine, take a look, and comment at will!

HOWTO - my from the trenches tech guides

MUSIC - without music, life would be a mistake

ART - I don't know where I'd be without it

POLITICS - the more things change...

http://fak3r.com/2011/10/12/linkedin-is-spamming-all-of-my-gmail-contacts

HOME ART GEEK MUSIC POLITICS ABOUT CONTACT SEARCH

« HOWTO install php5-fpm on Debian Squeeze

HOWTO run DD-WRT on a Netgear WNDR3700 »

LinkedIn is spamming all of my Gmail contacts

FAKER

look lout honey, cause I'm using technology

- so yes, I did opt-in
- but they didn't use the data in the manner I approved
- plus support didn't provide any help

UPDATE2 I finally got a response on Thu, Oct 27, 2011 at 7:24 AM, it said, "*I would first like to apologize for the [illegible] inquiry. This is certainly not the customary wait time for a reply [illegible] support. We have been experiencing higher than expected volumes, and your patience is greatly appreciated.*" So, they've been so busy that it took 2 1/2 weeks to get back to me. Oh, they have [illegible] questions, one what happened and two, who did they email on my behalf? I need a list. Stay tuned.

UPDATE today is October 17, 2011, so it's been a week since I've reported my problem, and I have not gotten anything back from LinkedIn support. Pathetic.

Move along nothing to see here

Here are some recommended categories of mine, take a look, and comment at will!

HOWTO - my from the trenches tech guides

MUSIC - without music, life would be a mistake

ART - I don't know where I'd be without it

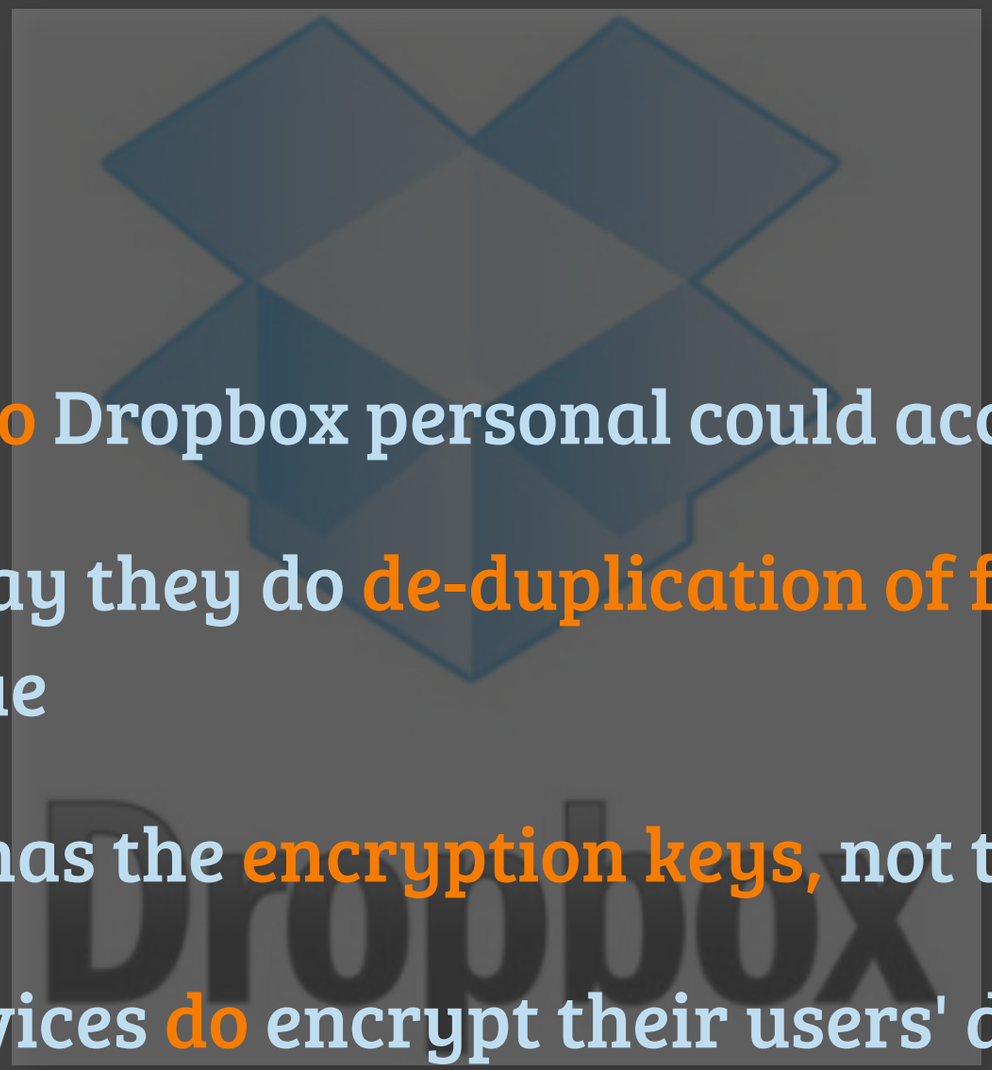
POLITICS - the more things change...

http://fak3r.com/2011/10/12/linkedin-is-spamming-all-of-my-gmail-contacts

…and let's not forget about file sharing

http://www.dropbox.com

How Dropbox sacrifices user privacy for cost savings



- claimed no Dropbox personal could access your files
- but the way they do de-duplication of files proved this wasn't true
- Dropbox has the encryption keys, not the user
- other services do encrypt their users' data with a key only known to the user

http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html

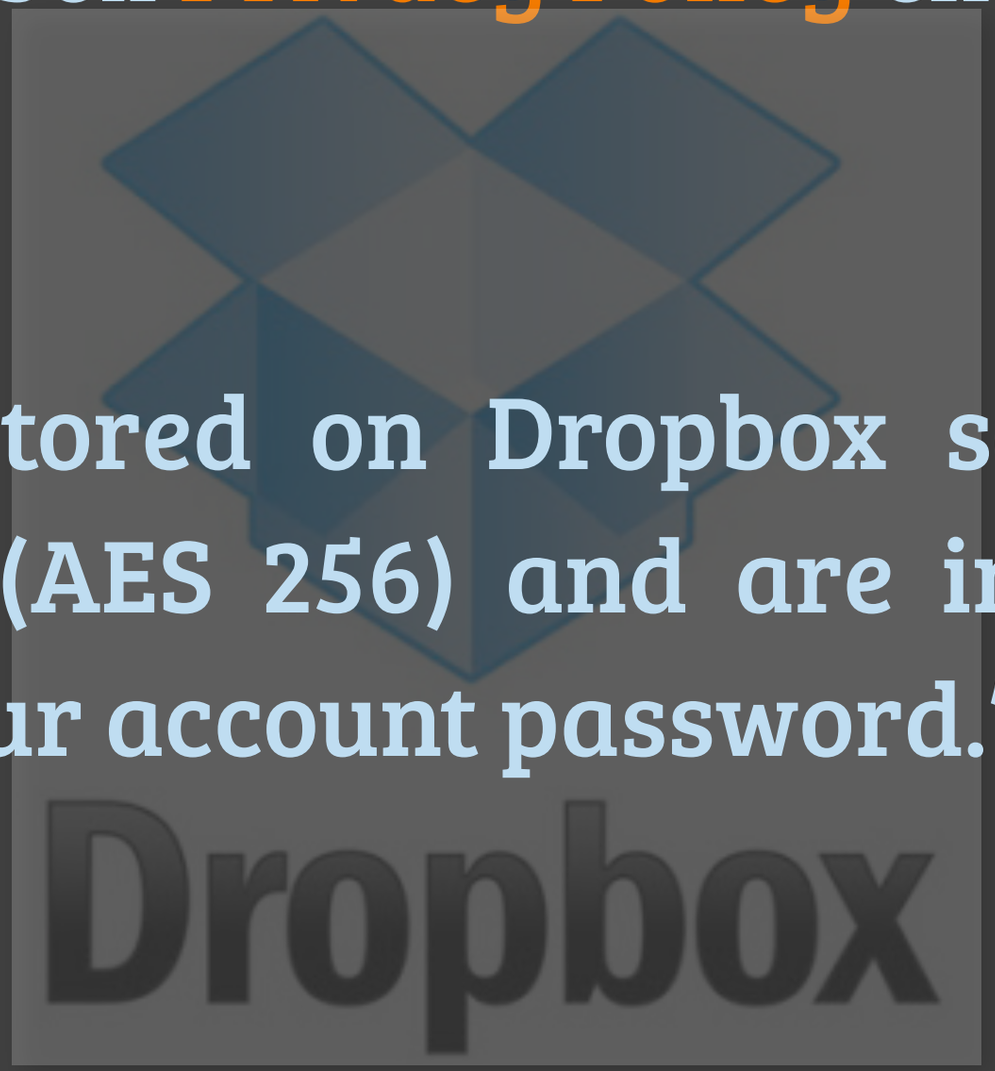
How Dropbox sacrifices user privacy for cost savings

On April 1, 2011, Marcia Hofmann at the Electronic Frontier Foundation contacted Dropbox to let them know about the flaw, and that a researcher would be publishing the information on April 12th.

At 6:15PM west coast time on April 11th, an attorney from Fenwick & West retained by Dropbox left Marcia a voicemail message, in which he reveled that: "the company is updating their privacy policy and security overview that is on the website to add further detail."

http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html

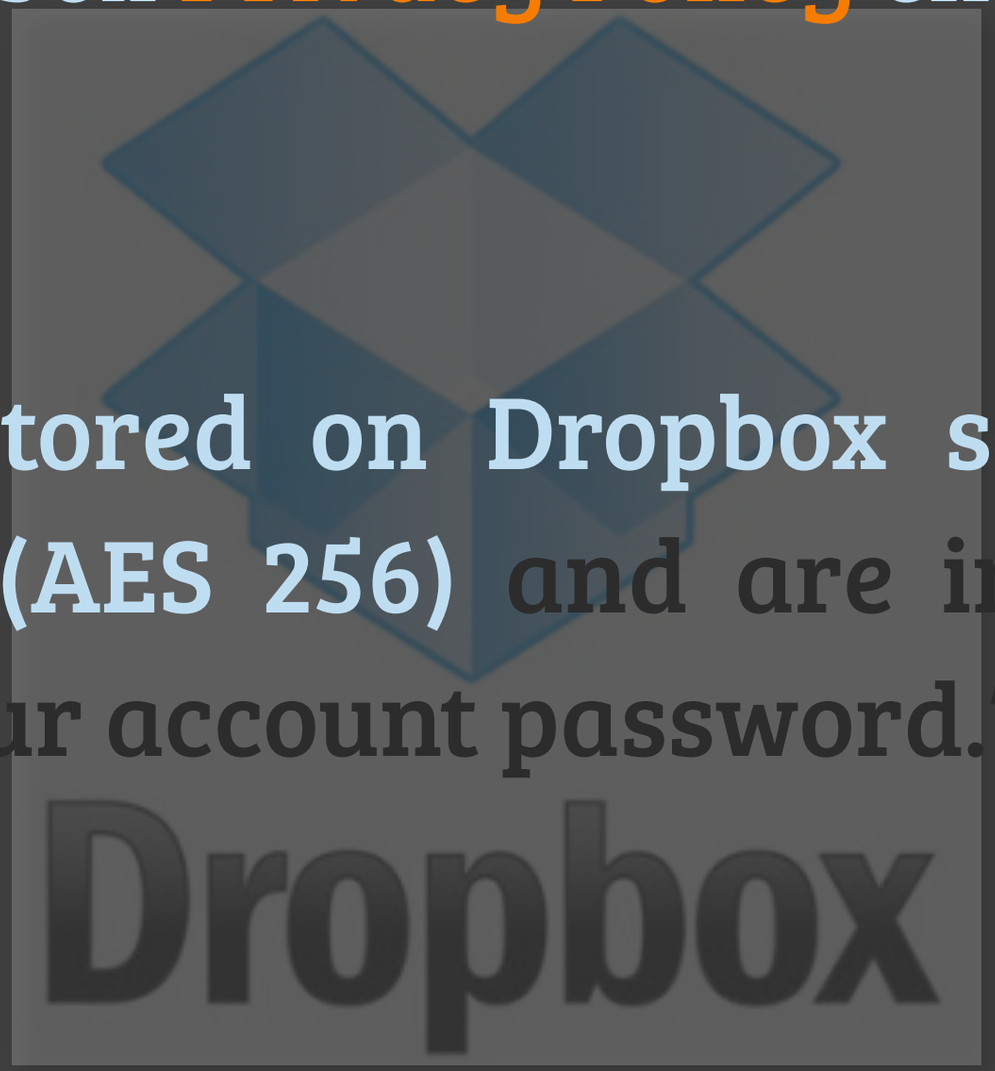
Dropbox Privacy Policy change



"All files stored on Dropbox servers are encrypted (AES 256) and are inaccessible without your account password."

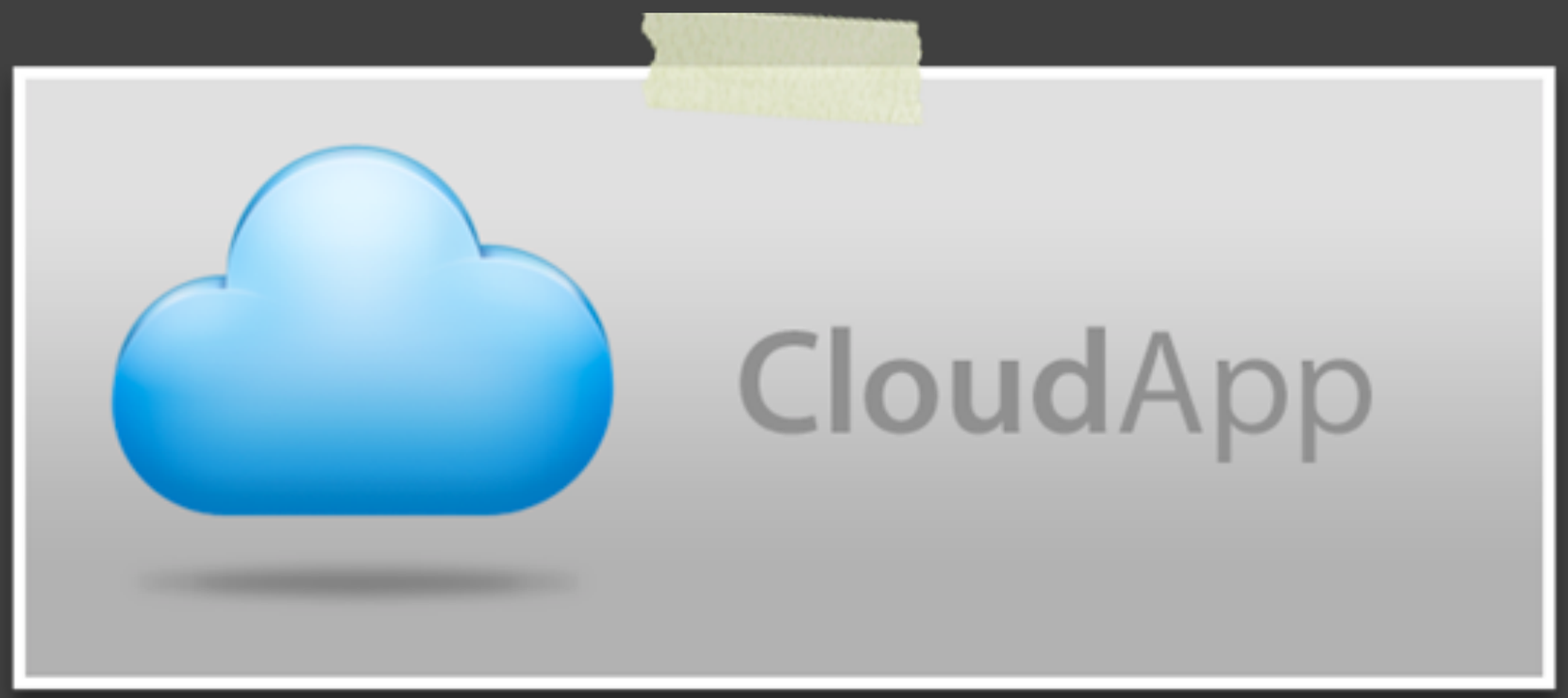
http://www.dropbox.com

Dropbox Privacy Policy change

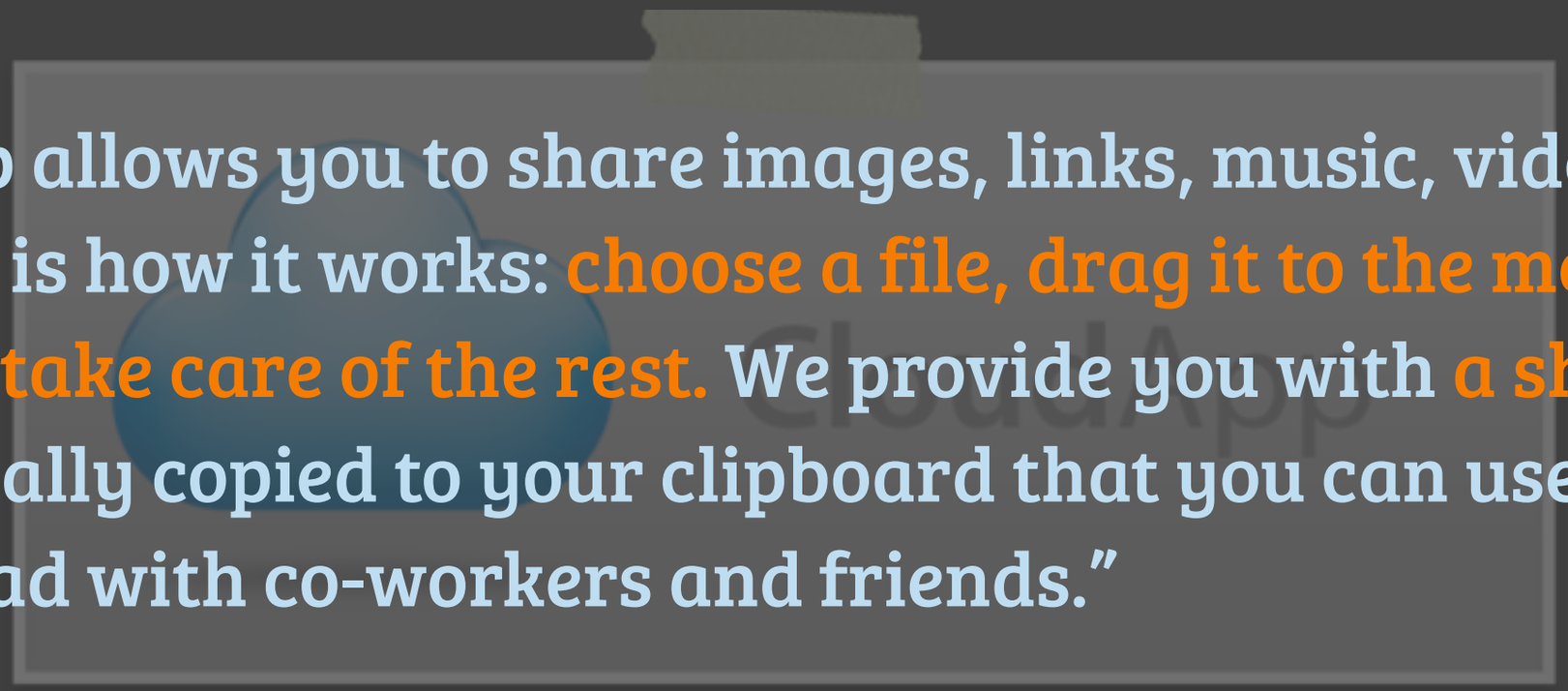


"All files stored on Dropbox servers are encrypted (AES 256) and are inaccessible without your account password."

http://www.dropbox.com



http://getcloudapp.com

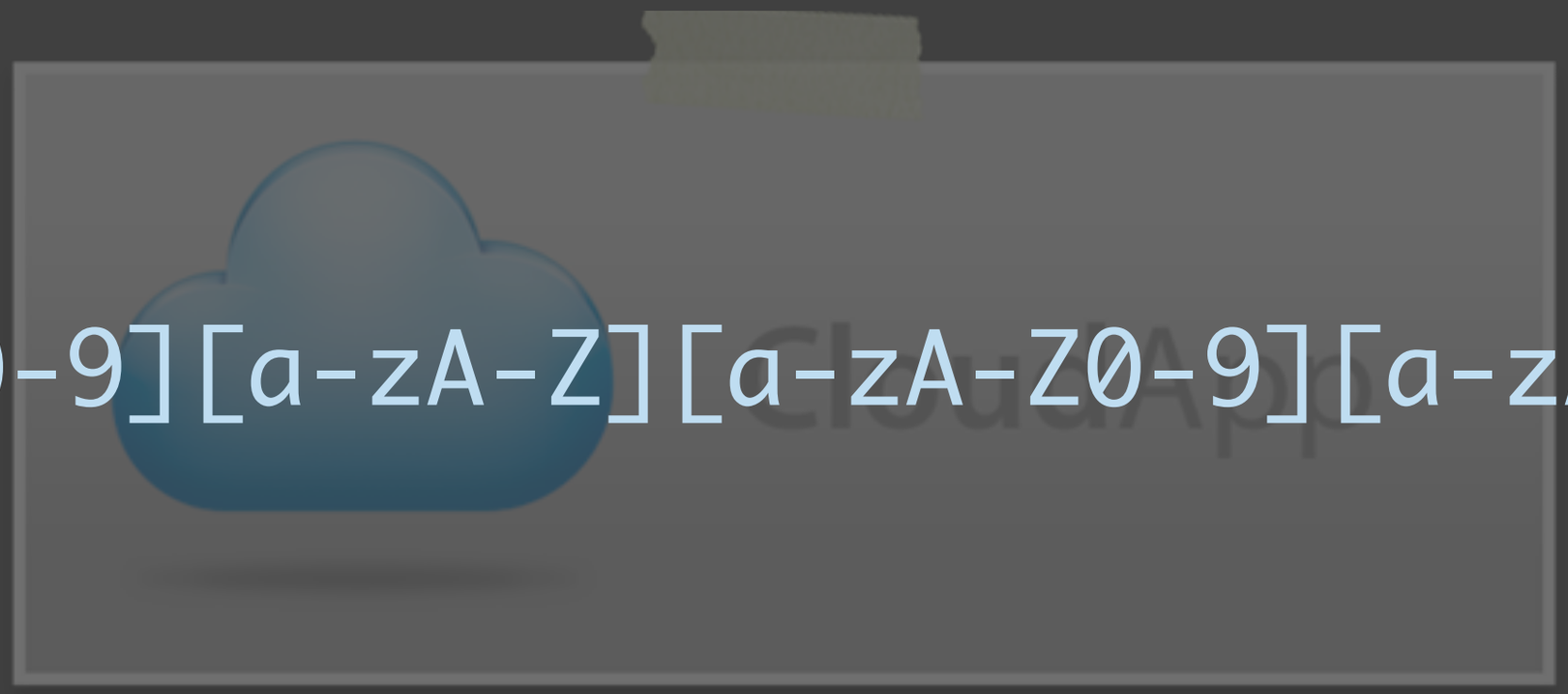


"CloudApp allows you to share images, links, music, videos and files. Here is how it works: choose a file, drag it to the menubar and let us take care of the rest. We provide you with a short link automatically copied to your clipboard that you can use to share your upload with co-workers and friends."

http://getcloudapp.com

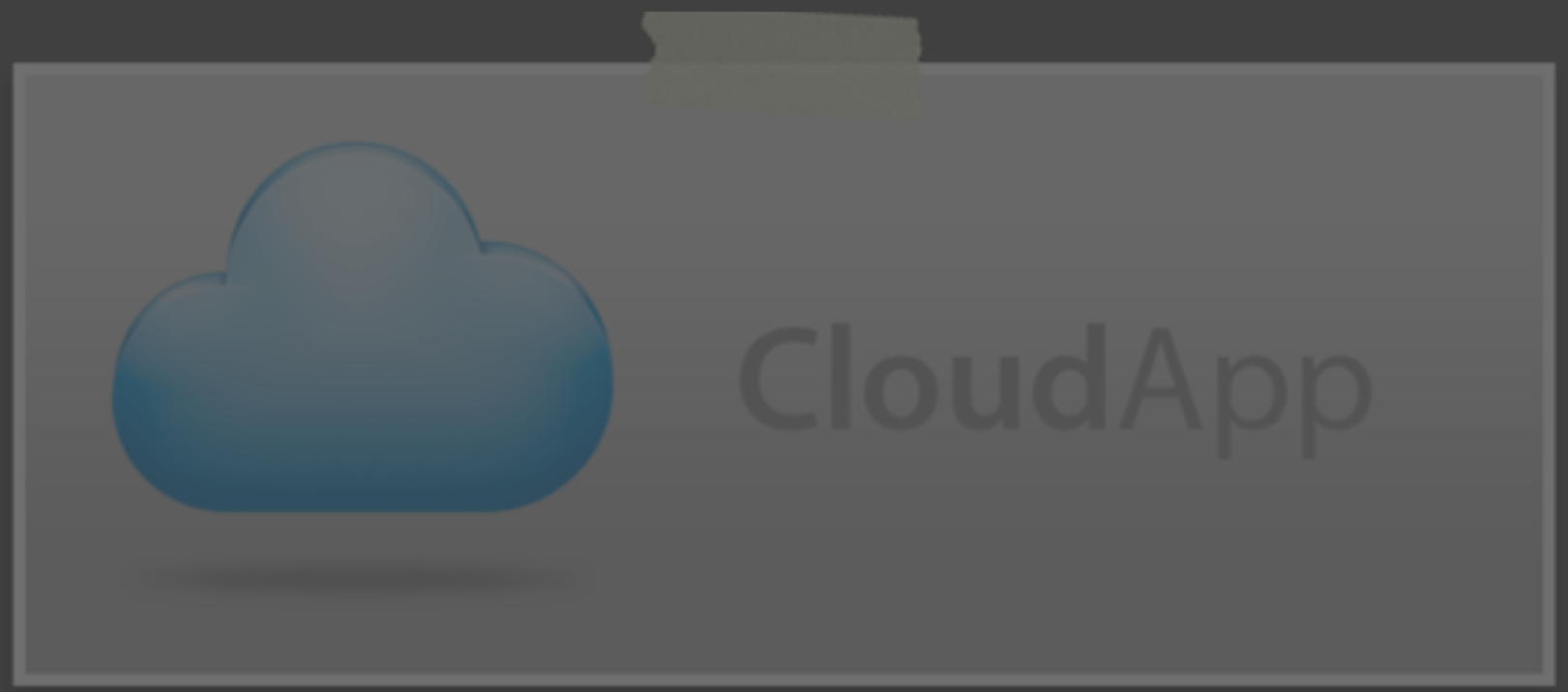
Unfortunately the weak entropy of characters used for their shortened URLs leads to (very) low privacy

http://getcloudapp.com



```
\/[0-9][a-zA-Z][a-zA-Z0-9][a-zA-Z]
```

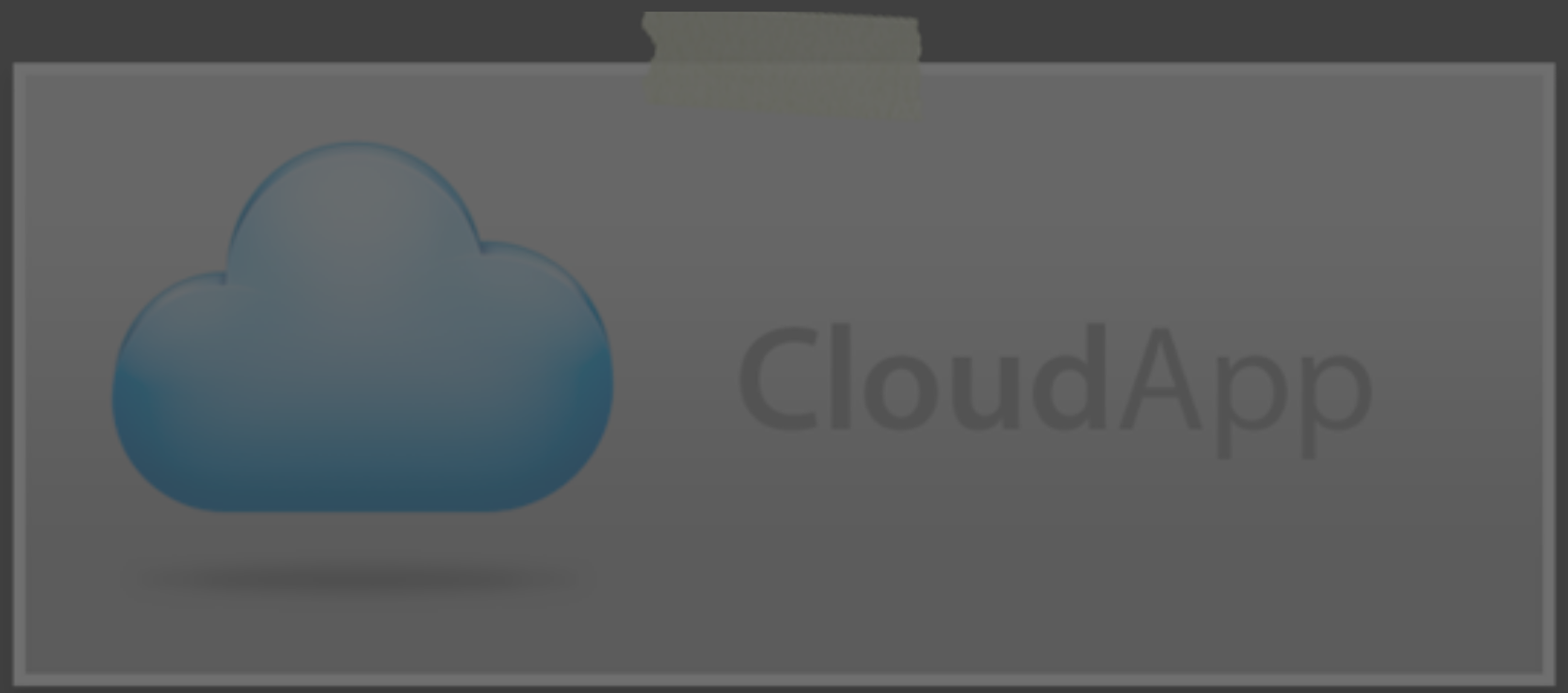
http://cl.ly/2a3e



http://getcloudapp.com

http://cl.ly/2a3e

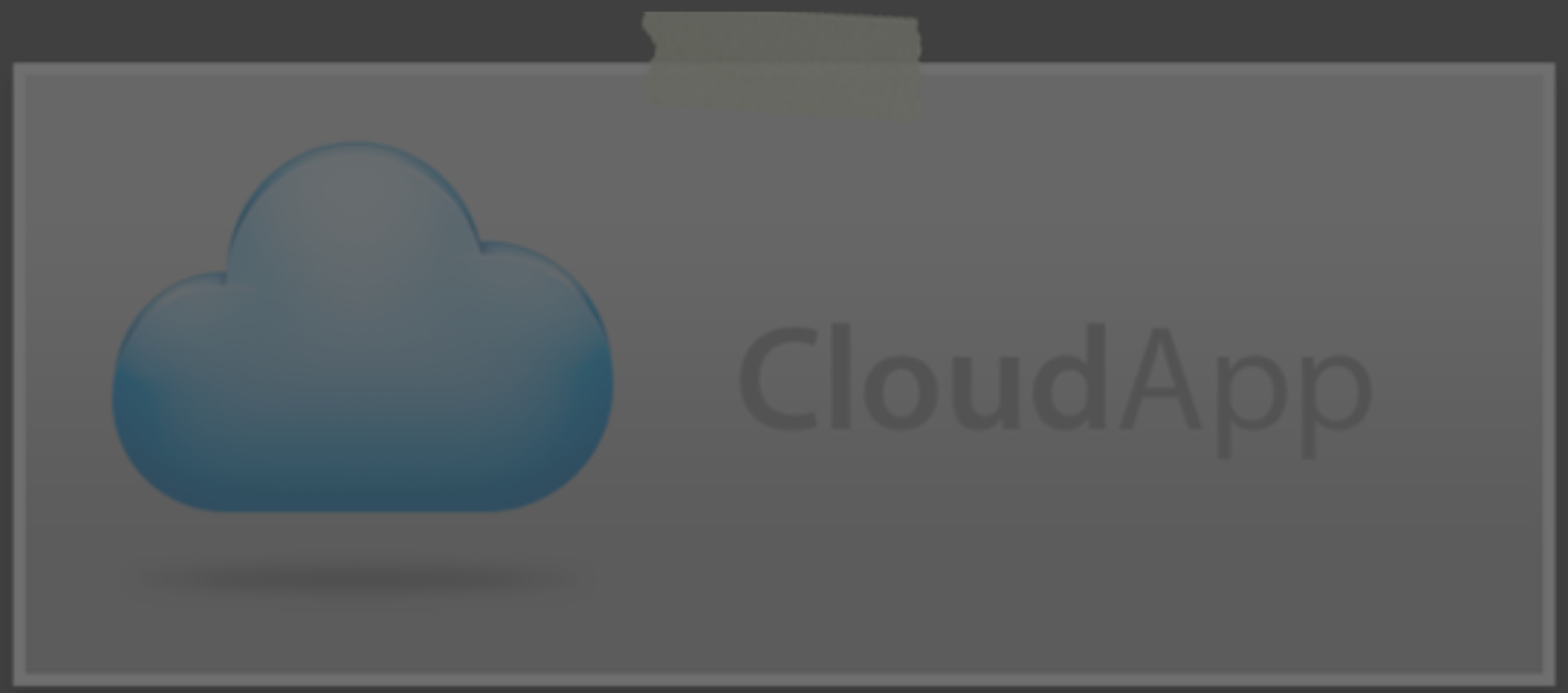
http://cl.ly/3l1k



http://getcloudapp.com

http://cl.ly/3l1k

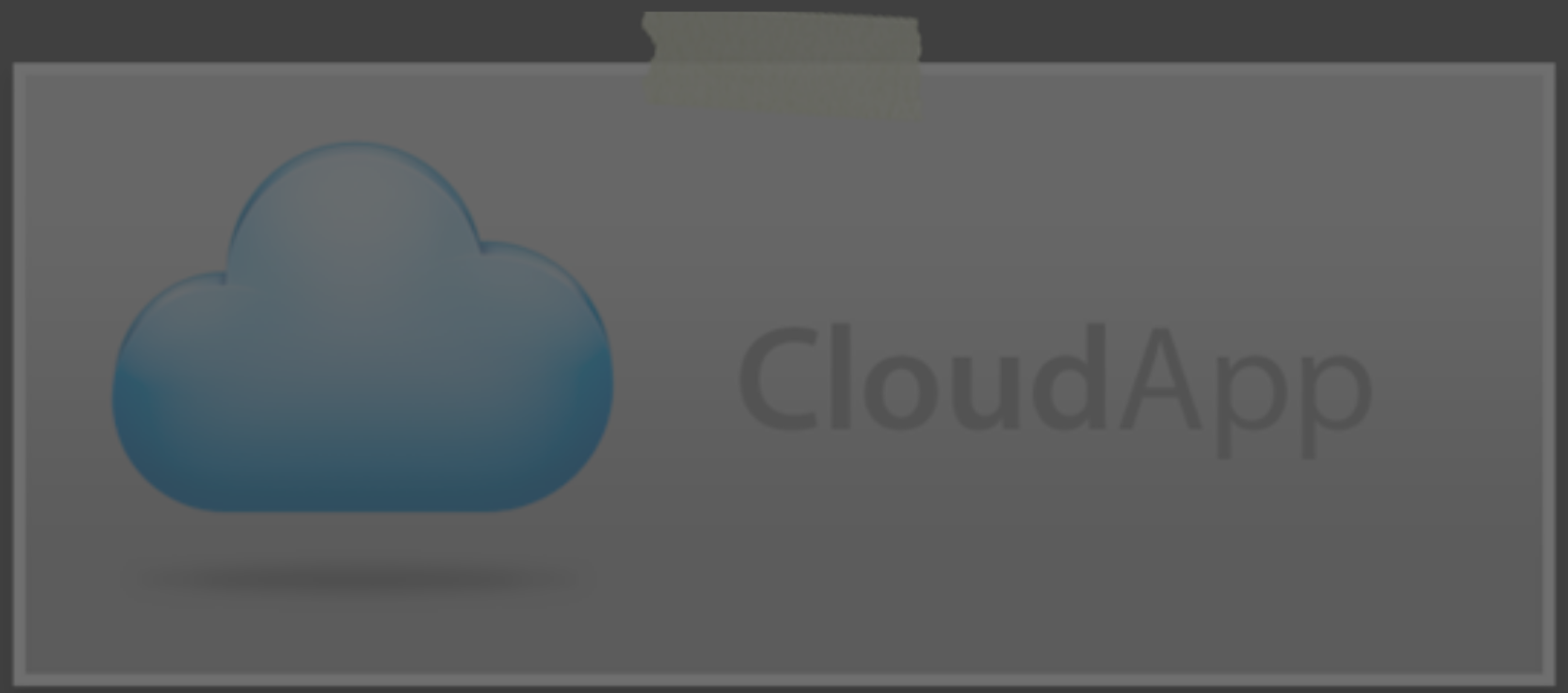
http://cl.ly/4g8d



http://getcloudapp.com

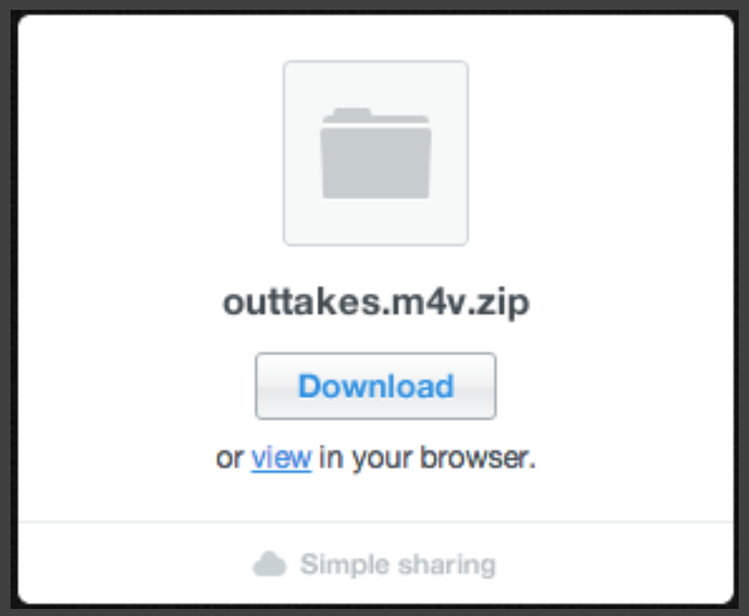
http://cl.ly/4ety

http://cl.ly/4ety

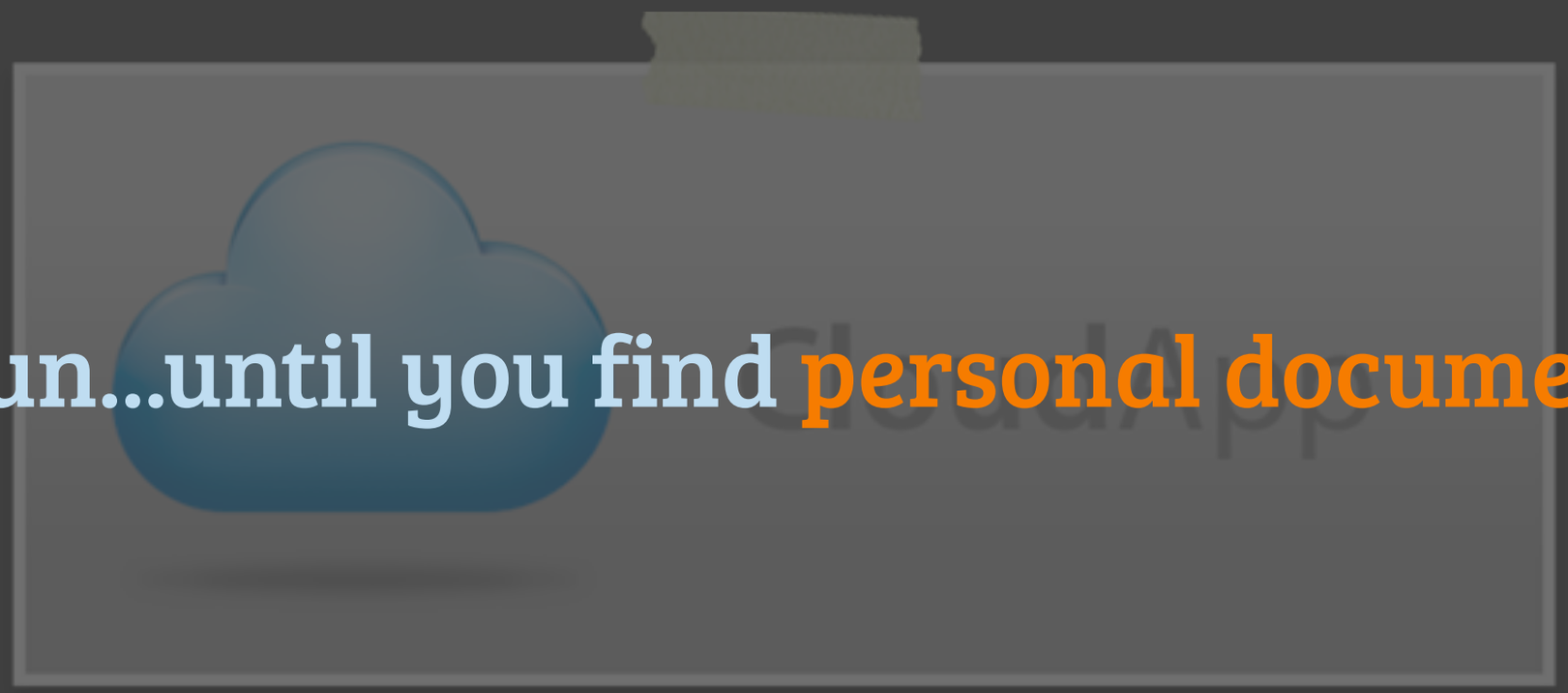


http://getcloudapp.com

http://cl.ly/4g8d



http://getcloudapp.com



This is fun...until you find personal documents

I wrote a script that can randomly download gigabytes of users' data, by guessing, or "brute forcing" different URL combinations

- plenty of pictures, mp3s, graphics
- credit card receipts, court documents, W9 forms, personal emails, Facebook posts, instant messages, passport scans
- ...and everything was unencrypted

People don't know they're sharing this data.

Responsible Disclosure: I reported my findings to CloudApp, they said they have a notice on their site that it may not be secure... but they still allow this kind of convenient 'sharing'

I have released the script to demonstrate this vulnerability.

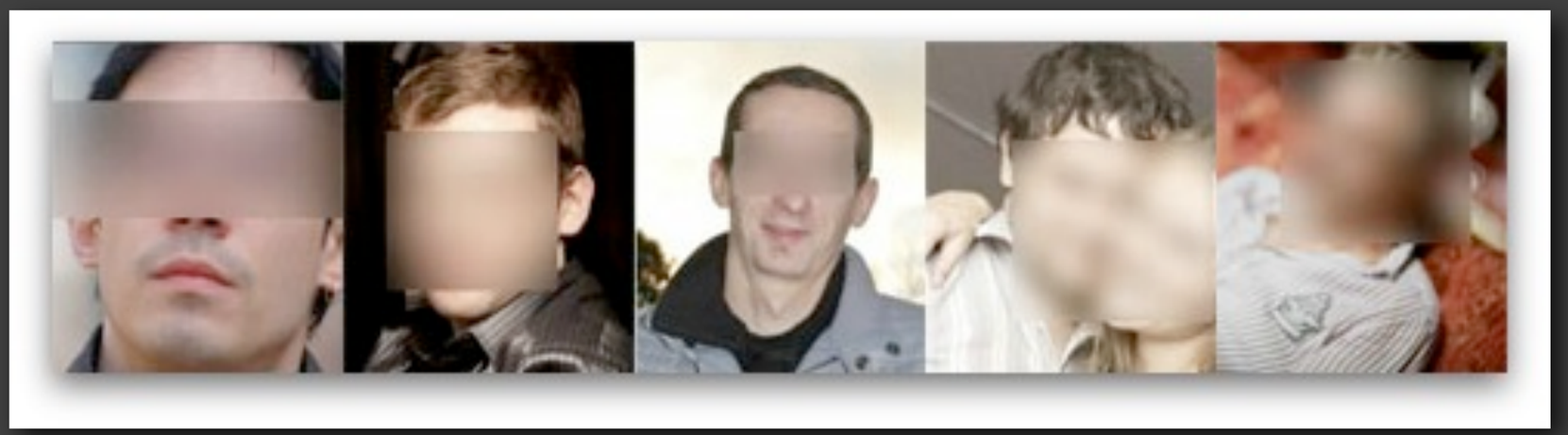
https://github.com/philcryer/ca-harvester

COMPANIES ARE NOT GOING TO LOOK OUT FOR, OR PROTECT, YOUR DATA

How else could all of this social media data be used?

To fight crime

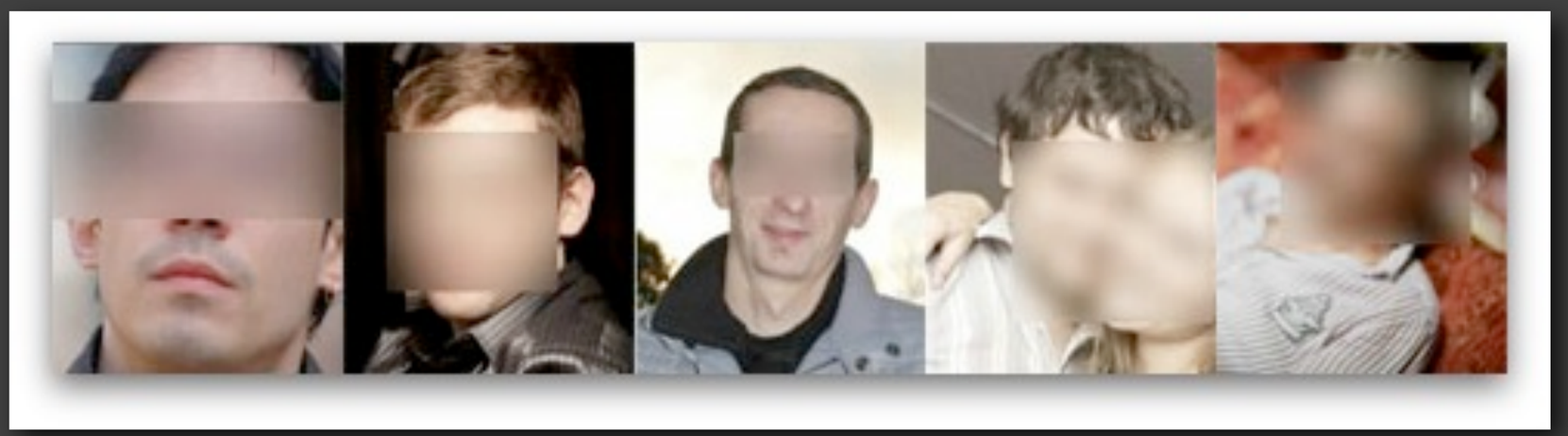
Facebook Unmasks Koobface Gang (P2P botnets) Aided By Their Foursquare Check-ins And Social Networking Photos



http://www.forbes.com/sites/kashmirhill/2012/01/17/facebook-unmasks-koobface-gang-aided-by-their-foursquare-check-ins-and-social-networking-photos

Facebook Unmasks Koobface Gang (P2P botnets) Aided By Their Foursquare Check-ins And Social Networking Photos

"...security researchers and members of the Facebook security team tracked digital breadcrumbs to expose the five men responsible for Koobface [...] they tracked them down based on IP fingerprints, Foursquare check-ins, Twitter activity, friend lists on a Russian social networking site, Flickr photos showing the gang vacationing across Europe."



http://www.forbes.com/sites/kashmirhill/2012/01/17/facebook-unmasks-koobface-gang-aided-by-their-foursquare-check-ins-and-social-networking-photos

For good, humanitarian purposes

Twitter Tracks Cholera Outbreaks Faster Than Health Authorities

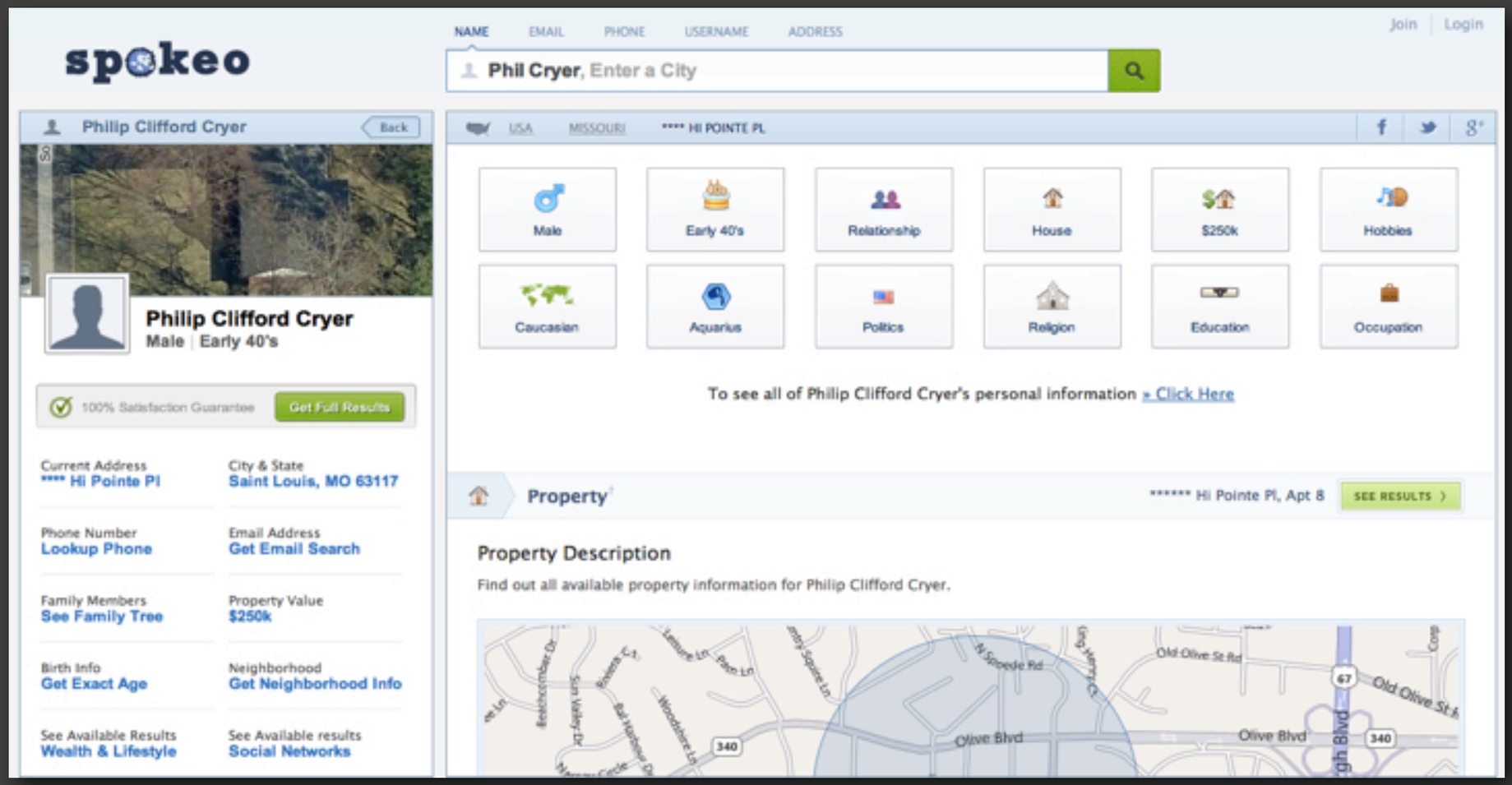
Now researchers have shown that, for the 2010 cholera epidemic in Haiti, social media like Twitter can track outbreaks as much as two weeks sooner than official health reports, especially when used by people with mobile phones.

http://chronicle.com/blogs/percolator/twitter-tracks-cholera-outbreaks-faster-than-health-authorities/28205

For nefarious purposes

https://xkcd.com
http://sylviamoessinger.wordpress.com/2011/05/04/h807-online-privacy-an-illusion-a10-1

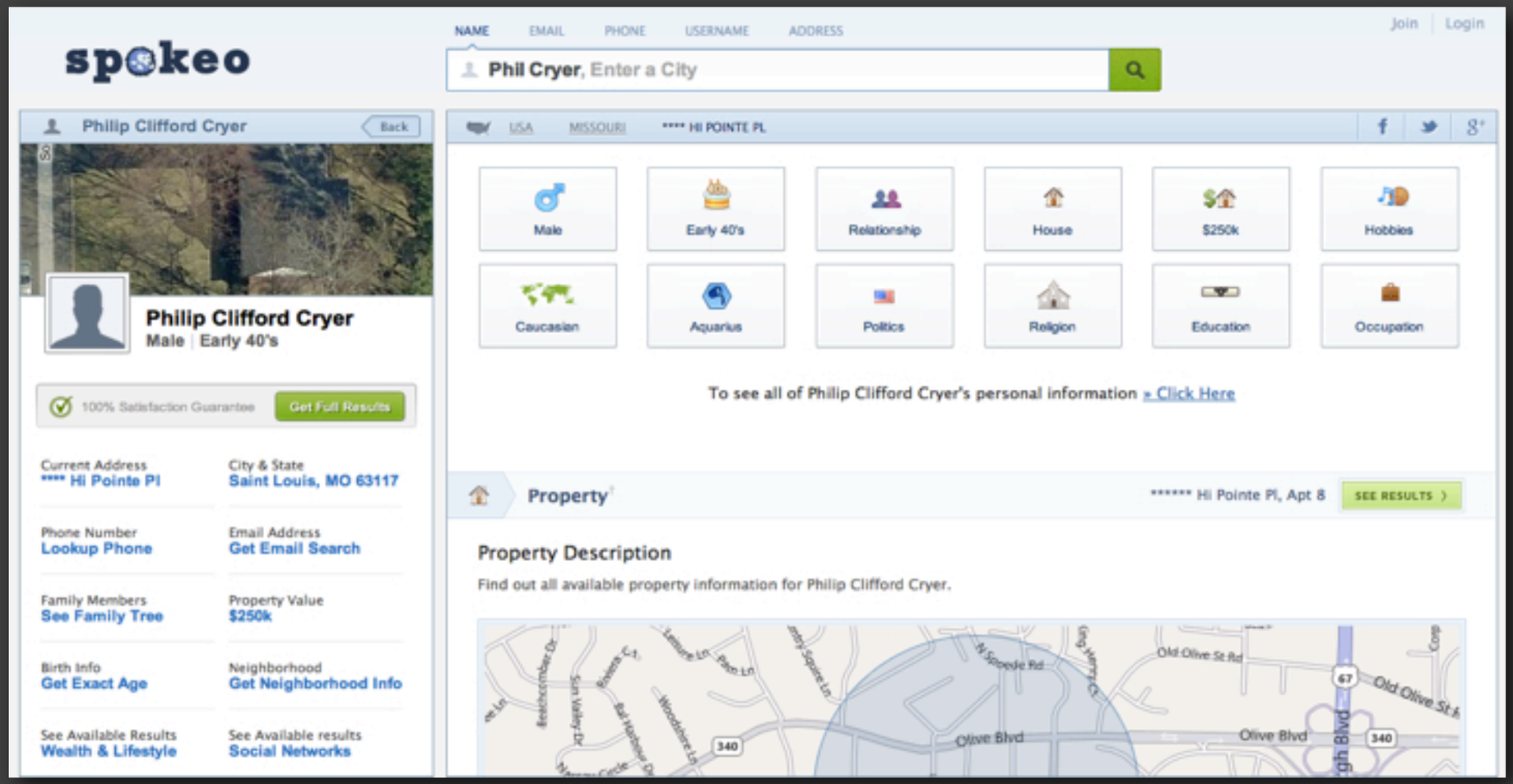
Spokeo is a people search engine



"...organizes vast quantities of white-pages listings, social information, and other people-related data from a large variety of public sources. Our mission is to help people find and connect with others, more easily than ever"

http://www.spokeo.com

Spokeo is a people search engine



"Not just Name, Age, Sex, but they also include Race, Politics, Religion, Cost of your home, Occupation, Education level, Salary, Hobbies... even your Zodaic sign" (?)

http://www.spokeo.com

UNDERSTAND WHY PRIVACY MATTERS

https://spideroak.com

http://zeroknowledgeprivacy.org/library/why-privacy-matters/

Communication Security; Riseup's primer on surveillance and security. Why security matters

- Because network surveillance is so pervasive, it is a social problem that affects everyone all the time. In contrast, device and message security are important for people who are being individually targeted by repressive authorities.
- Improving your network security is fairly easy, in comparison to device or message security.

https://help.riseup.net/en/security

The Right to Anonymity is a Matter of Privacy

- Privacy from employers
- Privacy from the political scene
- Privacy from the public eye
- Achieving anonymity online is a right

https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy

The Filter Bubble

"Internet firms increasingly show us less of the wide world, locating us in the neighborhood of the familiar. The risk, as Eli Pariser shows, is that each of us may unwittingly come to inhabit a ghetto of one."

http://bit.ly/filter-bubble

Why ‘I Have Nothing to Hide’ Is the Wrong Way to Think About Surveillance

WIRED

“If everyone’s every action were being monitored, and everyone technically violates some obscure law at some time, then punishment becomes purely selective. Those in power will essentially have what they need to punish anyone they’d like, whenever they choose, as if there were no rules at all. We’re not dealing with a balance of forces looking for the perfect compromise between security and privacy, but an enormous steam roller”

http://www.wired.com/opinion/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/

UNDERSTAND THAT PRIVATE BROWSING ISN'T PRIVATE

Private browsing isn't very private

The ONLY thing it does is keep people who go on your **actual, physical computer** from seeing the sites you've been to...

...but the **rest of the world** can see everything.

http://donottrackplus.com/learn/pbrowsing.php

KNOW WHAT YOU ARE SHARING

Block trackers before they get your information – social sites, ad networks, companies, (governments?)

Do Not Track Plus

Ghostery

https://www.ghostery.com
http://donottrack.us
http://donottrackplus.com

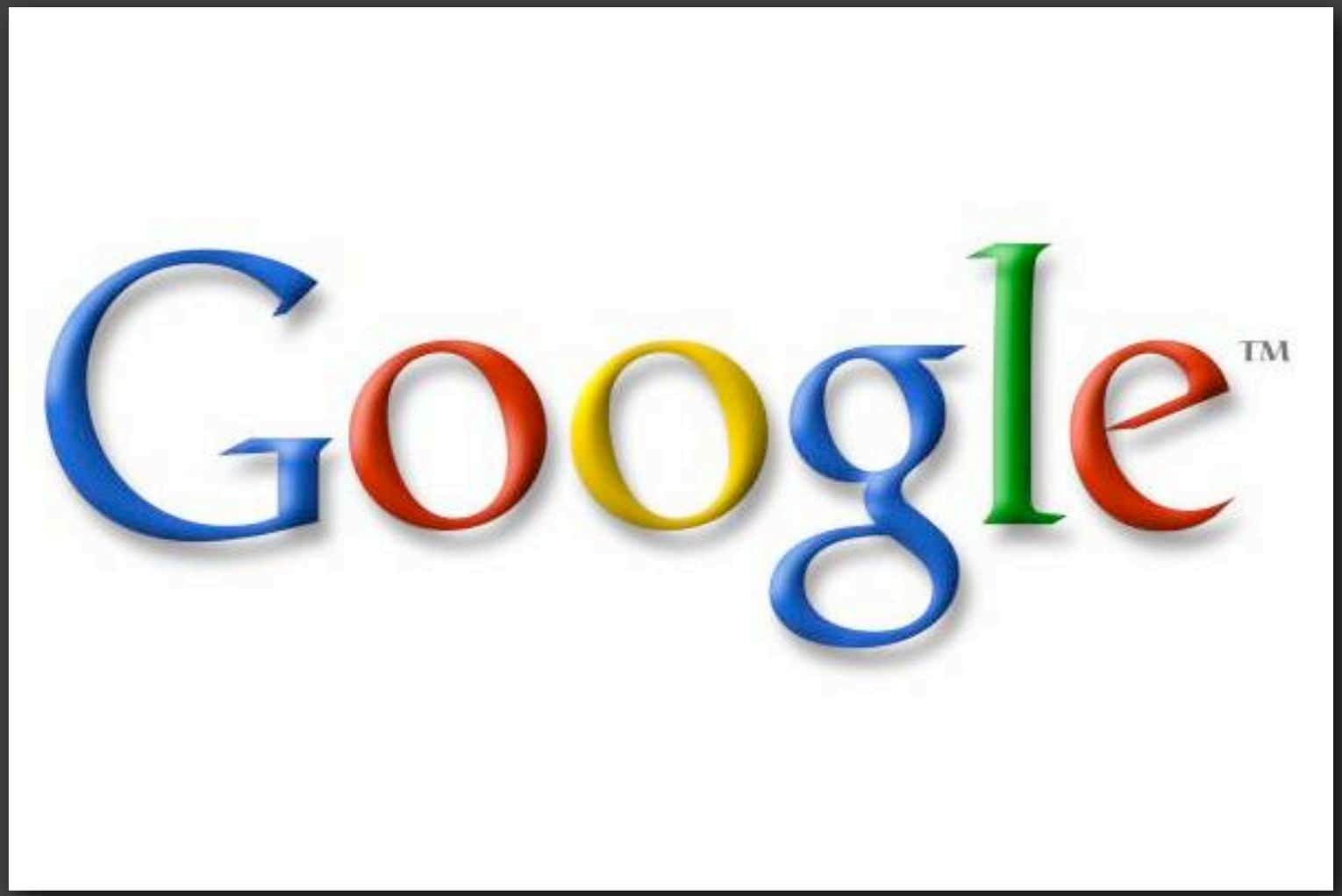
Blocks ads, flash and javascript trackers

http://noscript.net

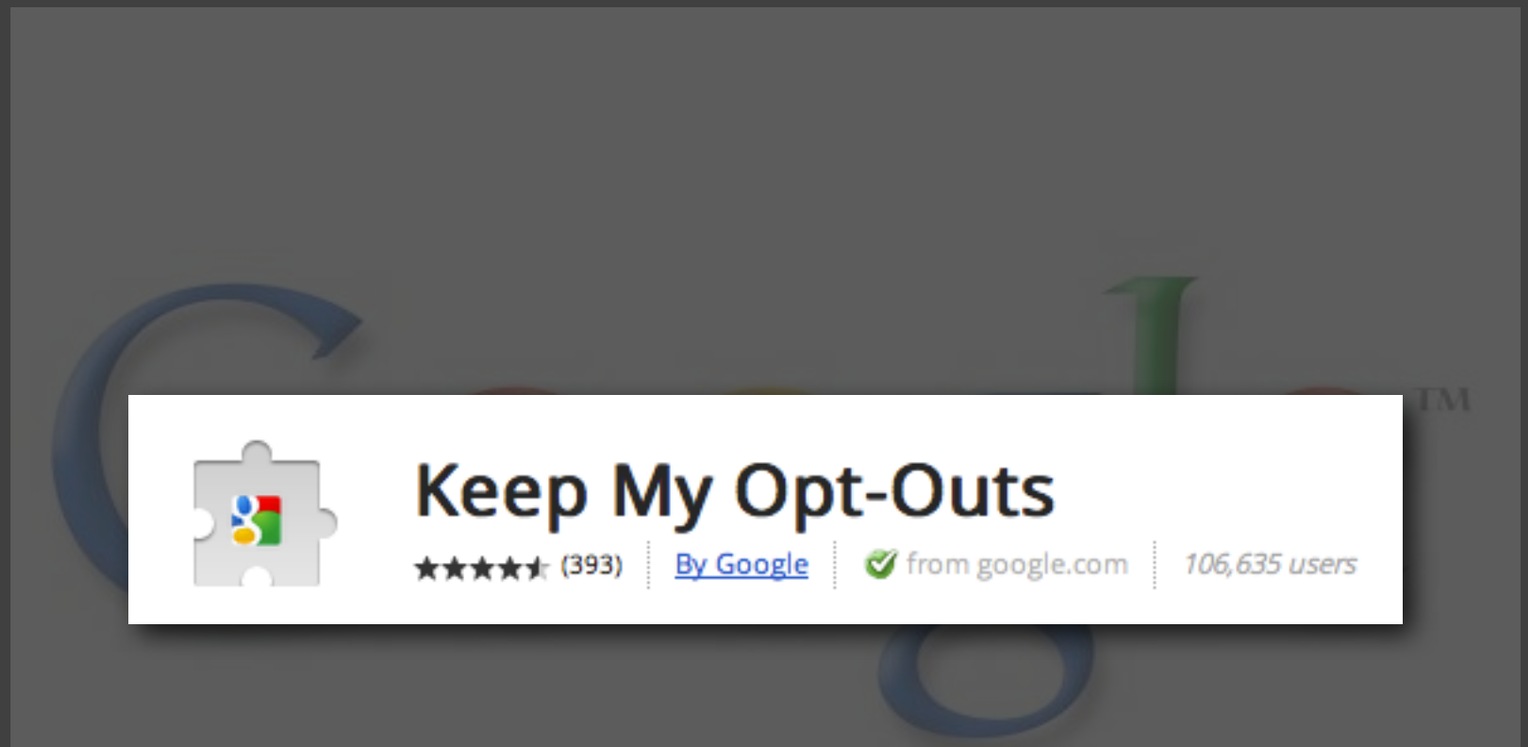
http://adblockplus.org

https://addons.mozilla.org/en-US/firefox/addon/flashblock

OPT-OUT OF SHARING


Google™

Via browser plugins



Download the advertising cookie opt-out plugin

Save your opt-out preference permanently with Google's plugin for your browser

Get Google Analytics Opt-out Browser Add-on (BETA)

Available for Internet Explorer (versions 7 and 8), Google Chrome (4.x and higher), and Mozilla Firefox (3.5 and higher).

http://google.com/settings/ads/onweb

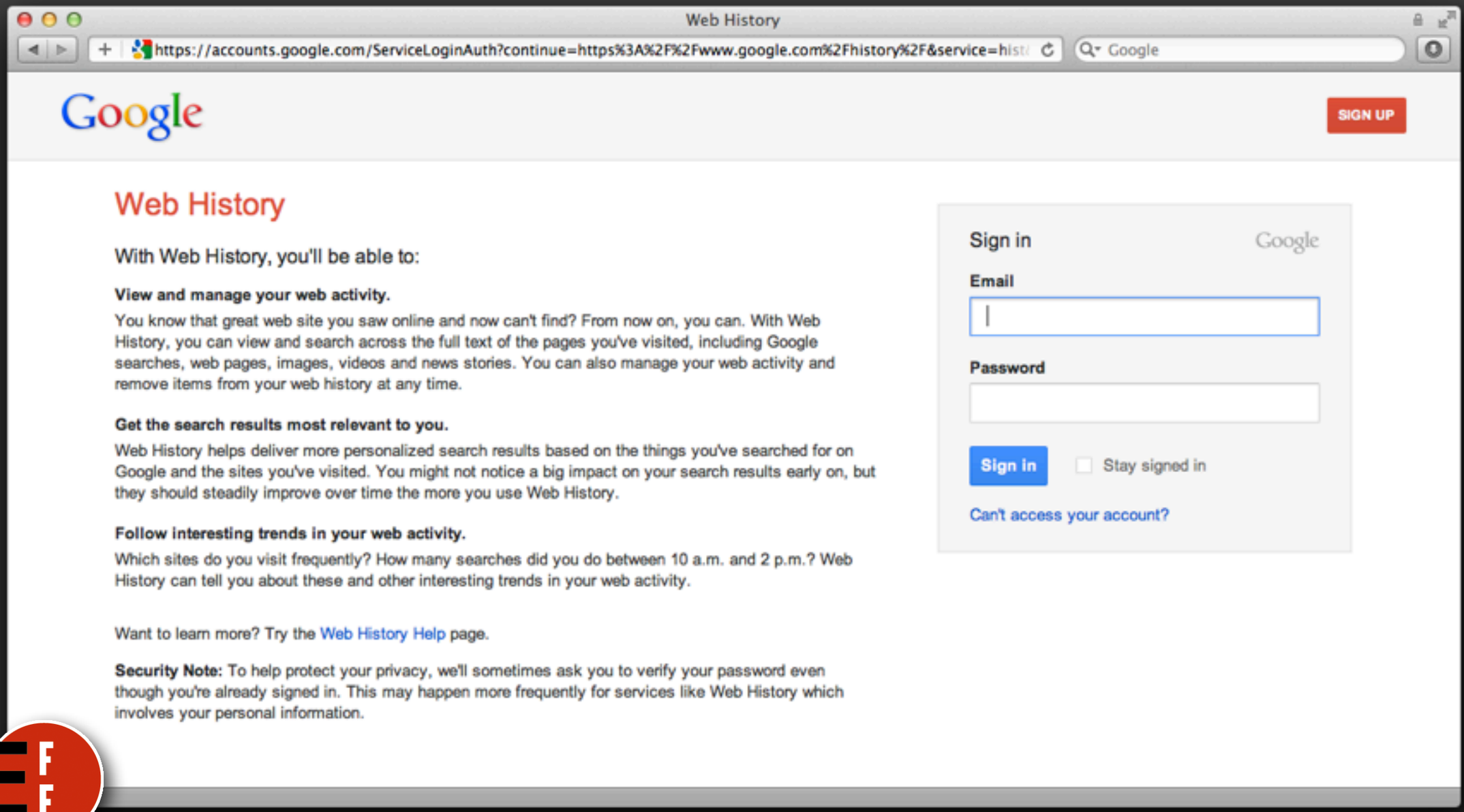
Or opt-out manually

http://bit.ly/optout

http://www.google.com/ads/preferences/plugin/browsers.html

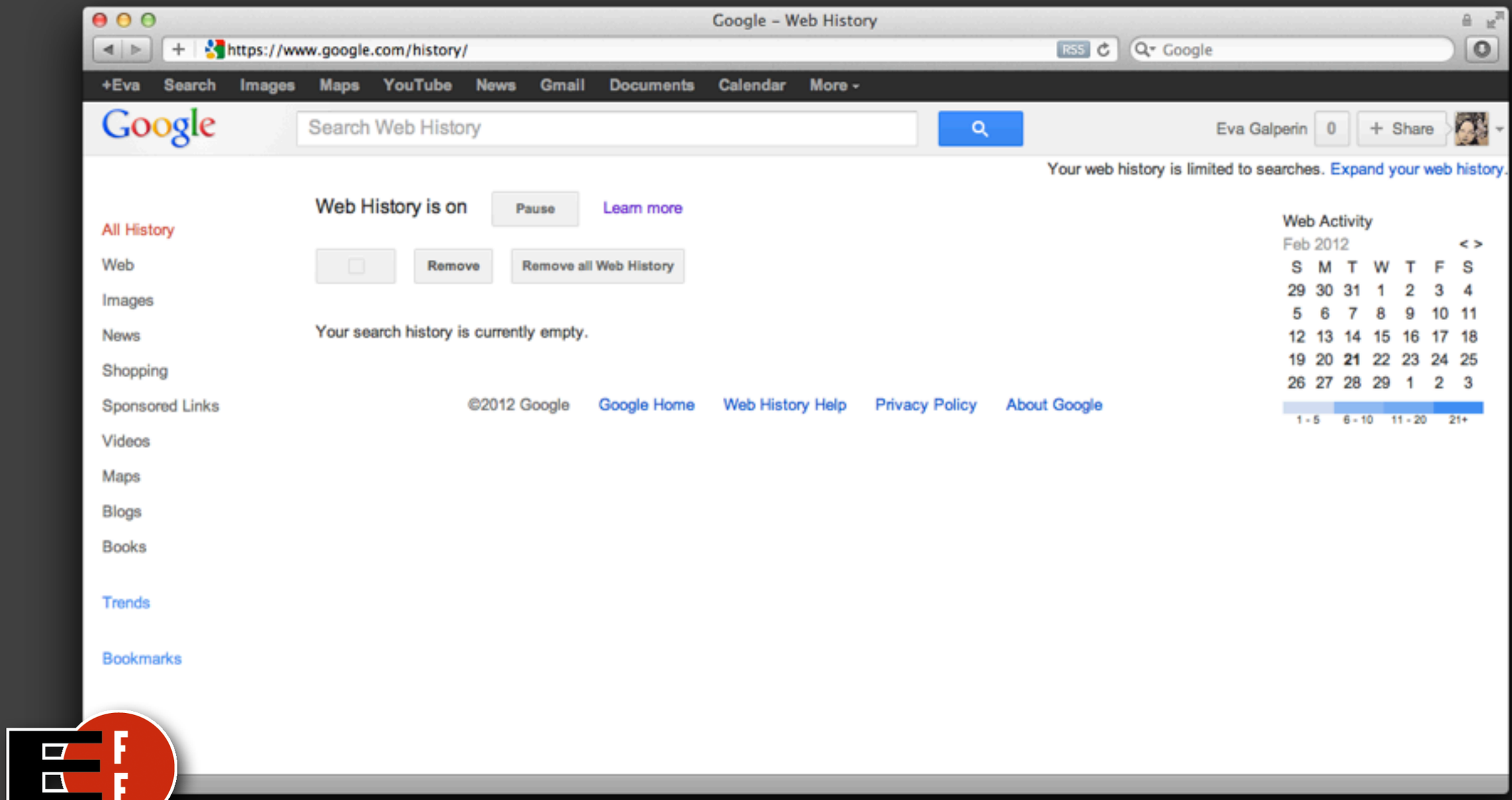
REMOVE YOUR GOOGLE SEARCH HISTORY

1 Sign into your Google account



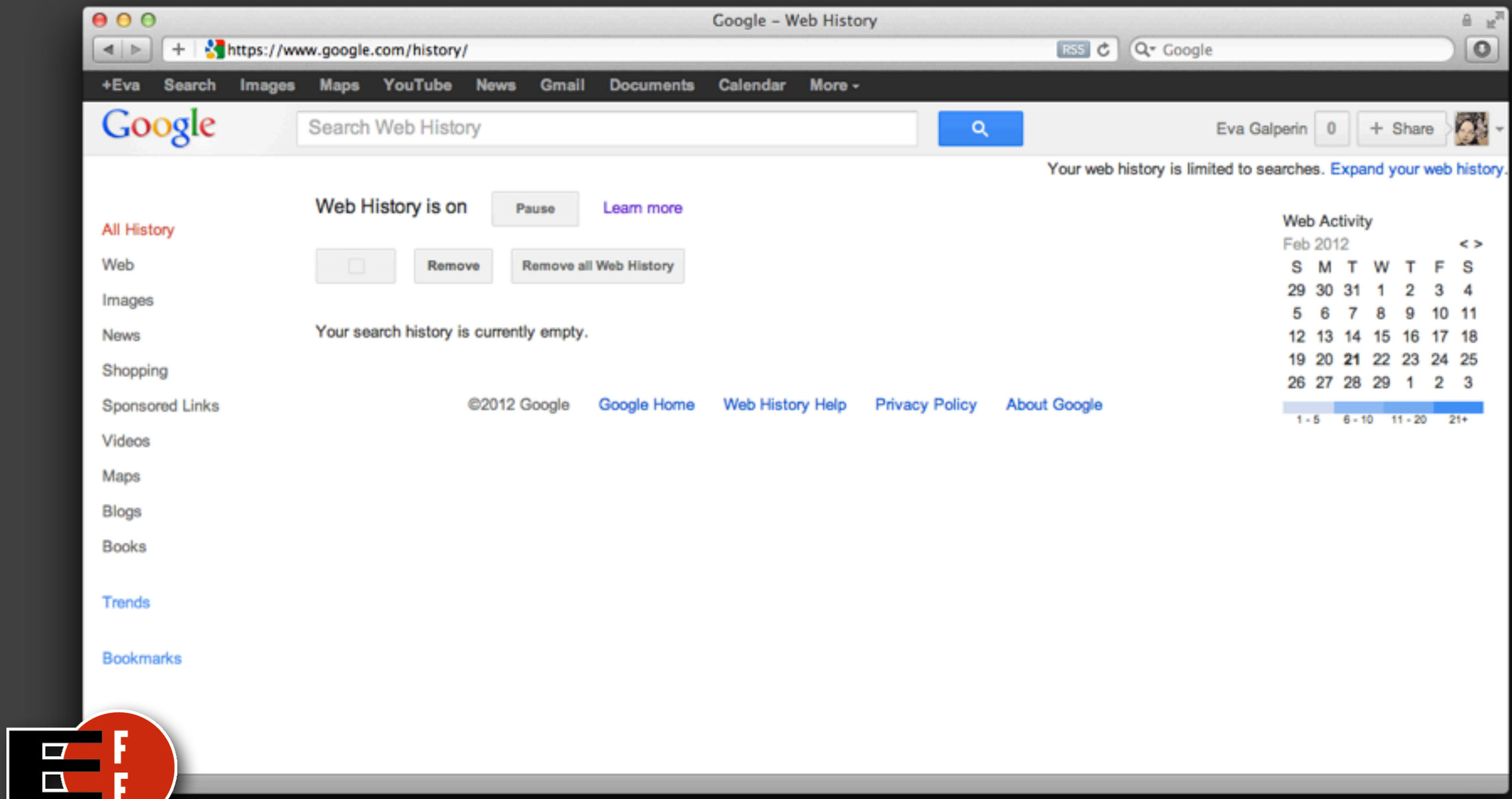
https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

2 Go to https://google.com/history



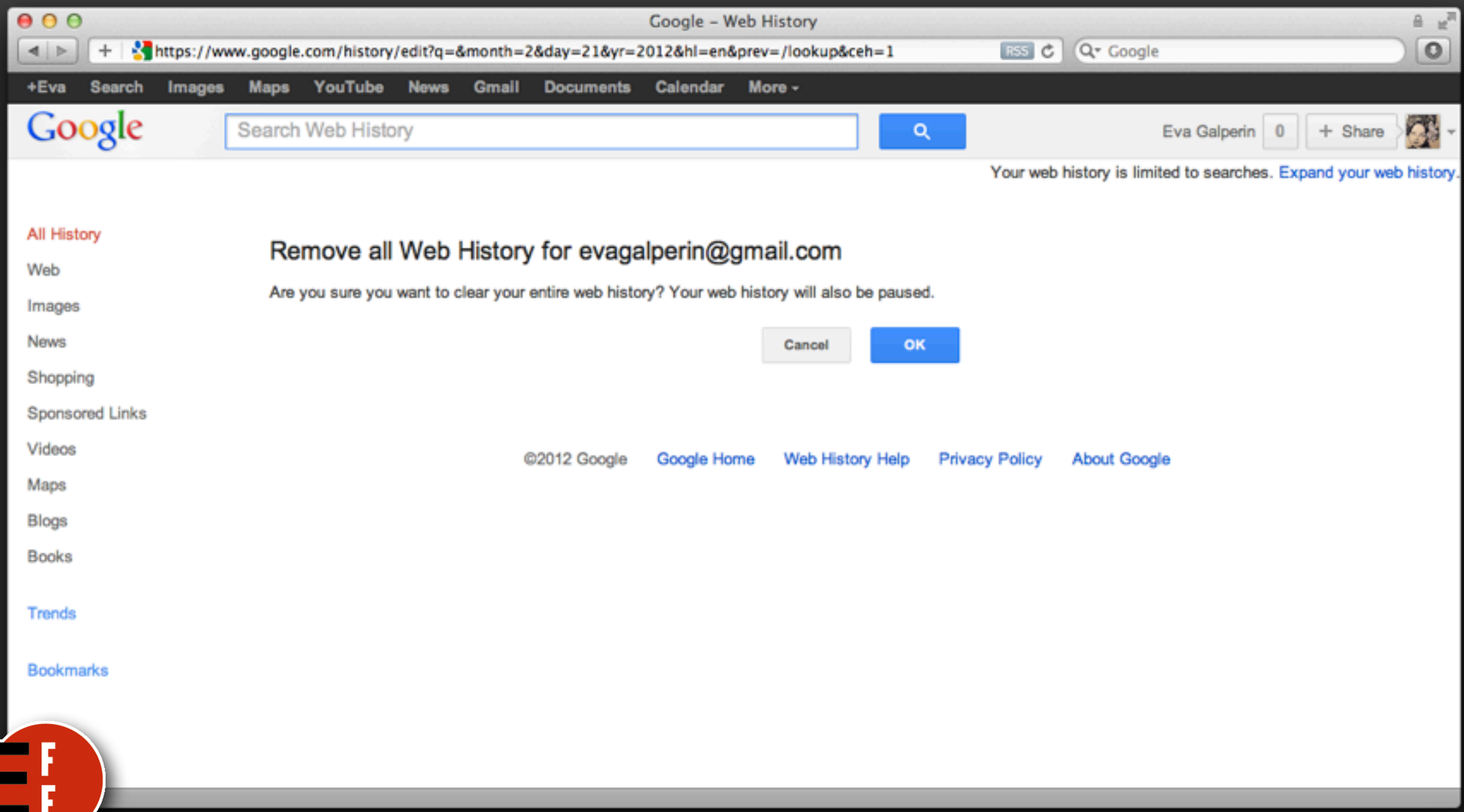
https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

3 Click "remove all Web History"



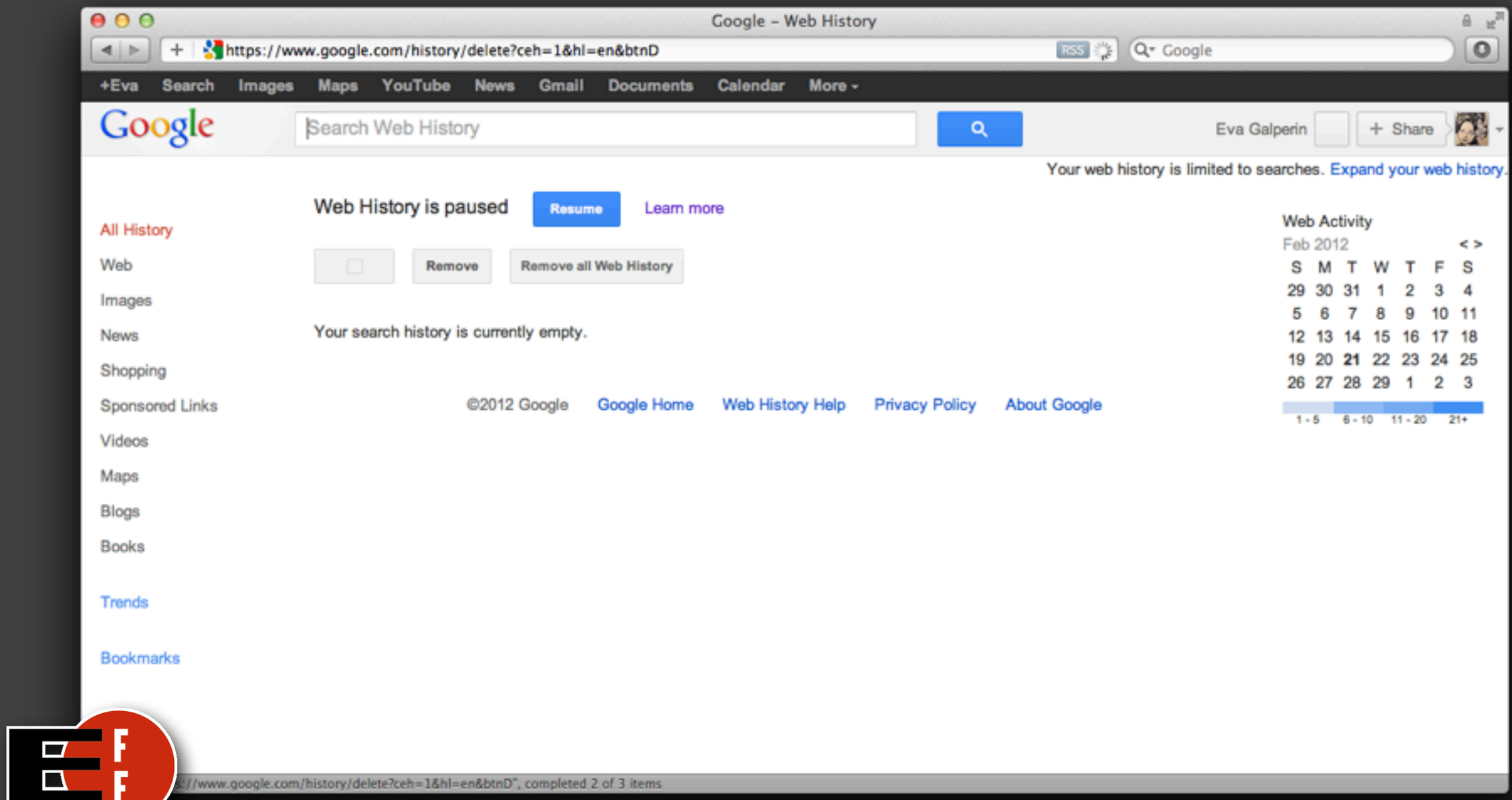
https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

4 Click "OK"



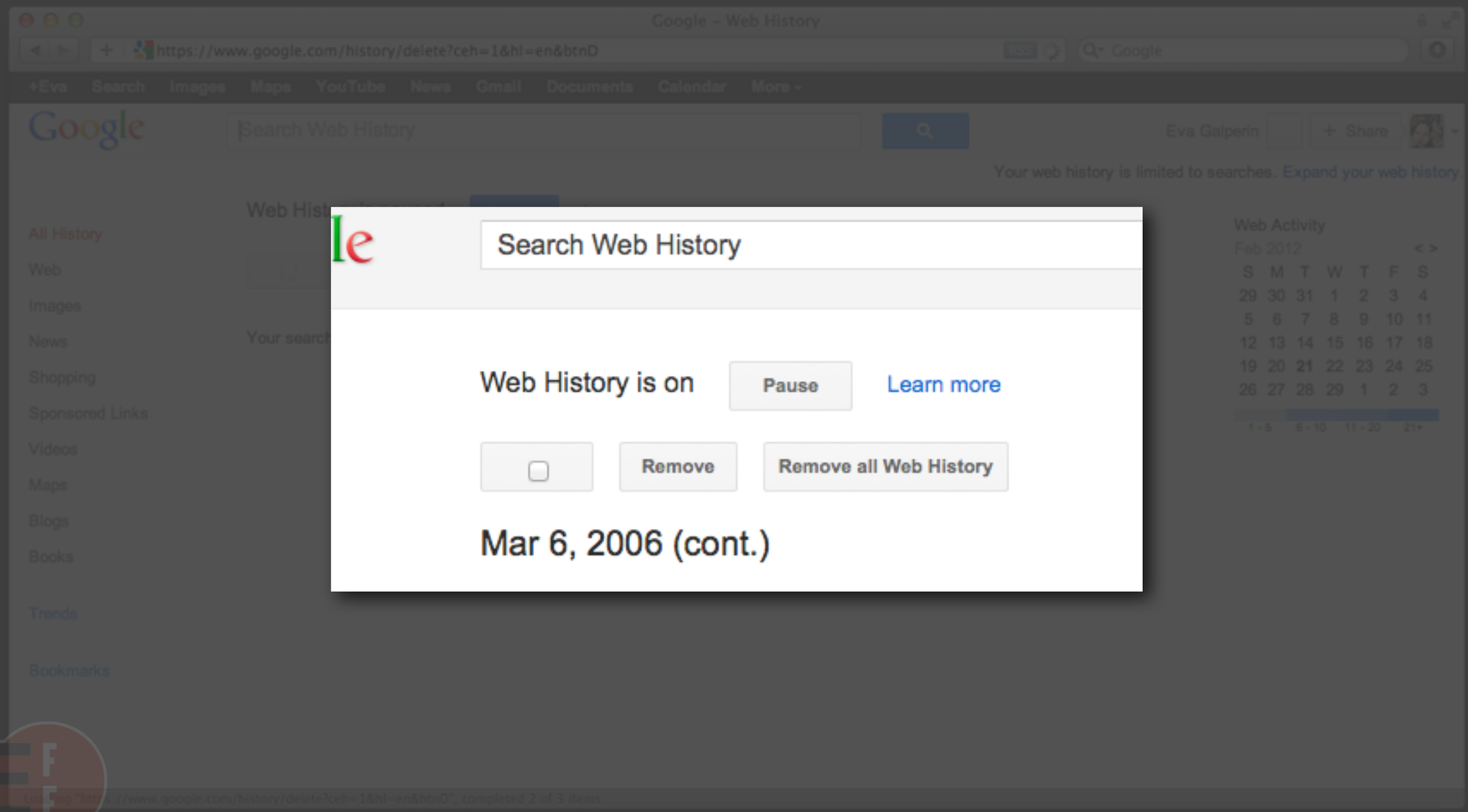
https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

This pauses web history, and it **will remain off until you enable it again,** but this won't stop Google's other tracking methods



https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

Oops, my history was saved back a few years :)



https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect

DON’T SHARE TOO MUCH

http://www.npr.org/blogs/thetwo-way/2013/06/17/192646711/cringe-miss-utah-fumbles-on-income-inequality-question?utm_source=npr&utm_medium=facebook&utm_campaign=20130617

?utm_source=npr
&utm_medium=face
book
&utm_campaign=20
130617

http://www.npr.org/blogs/thetwo-way/2013/06/17/192646711/cringe-miss-utah-fumbles-on-income-inequality-question

http://www.theonion.com/video/nation-demands-new-photograph-of-edward-snowden,32831/?utm_source=Facebook&utm_medium=SocialMarketing&utm_campaign=standard-post:other:default

?utm_source=Facebook
&utm_medium=SocialMa
rketing
&utm_campaign=standa
rd-post
:other
:default

http://www.theonion.com/video/nation-demands-new-photograph-of-edward-snowden,32831/

http://www.politico.com/story/2013/06/nsa-keith-alexander-cyber-shield-92880.html#.Ub9NiDLHxwA.twitter

#.Ub9NiDLHxwA.twitter

http://www.politico.com/story/2013/06/nsa-keith-alexander-cyber-shield-92880.html

BROWSE SECURELY

HTTPS is your friend

http://alexmillers.wordpress.com/2011/05/11/https-is-your-friend

HTTPS for the entire session. Why?

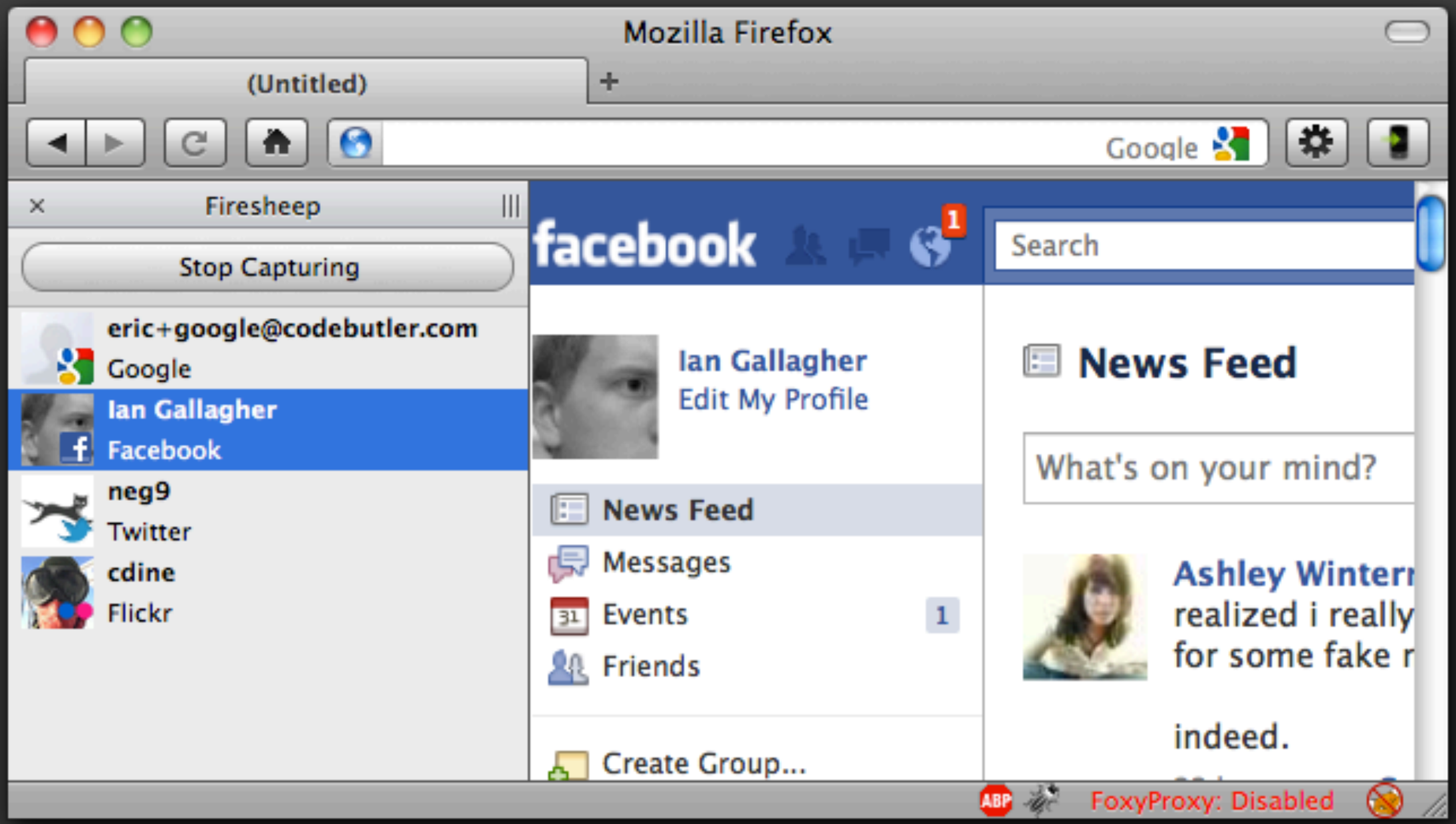
Session hijacking aka sidejacking

https://en.wikipedia.org/wiki/Session_hijacking

You login with https but then drops you to http

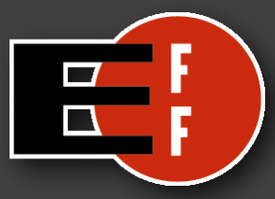
https://en.wikipedia.org/wiki/Session_hijacking

Firesheep


Mozilla Firefox
(Untitled)
Google
Firesheep
Stop Capturing
eric+google@codebutler.com
Google
Ian Gallagher
Facebook
neg9
Twitter
cdine
Flickr
facebook
1
Search
Ian Gallagher
Edit My Profile
News Feed
Messages
Events
1
Friends
Create Group...
News Feed
What's on your mind?
Ashley Winter
realized i really
for some fake r
indeed.
ABP
FoxyProxy: Disabled

HTTPS Everywhere

"HTTPS Everywhere is an extension for Firefox and Google Chrome, created by EFF and the Tor Project. It automatically switches thousands of sites from insecure "http" to secure "https". It will protect you against many forms of surveillance and account hijacking, and *some* forms of censorship"



https://www.eff.org/https-everywhere

ENCRYPT YOUR DNS QUERIES

DNSCrypt

"A tool for **securing communications between a client and a DNS resolver** [...] significant because it encrypts all DNS traffic between Internet users and OpenDNS*. This [...] thwarts efforts by attackers, MiTM, or even Internet Service Providers (ISPs), from **spying on DNS activity, or worse,** maliciously redirecting DNS traffic"

OpenDNS

* can be used with any DNS provider, not just OpenDNS

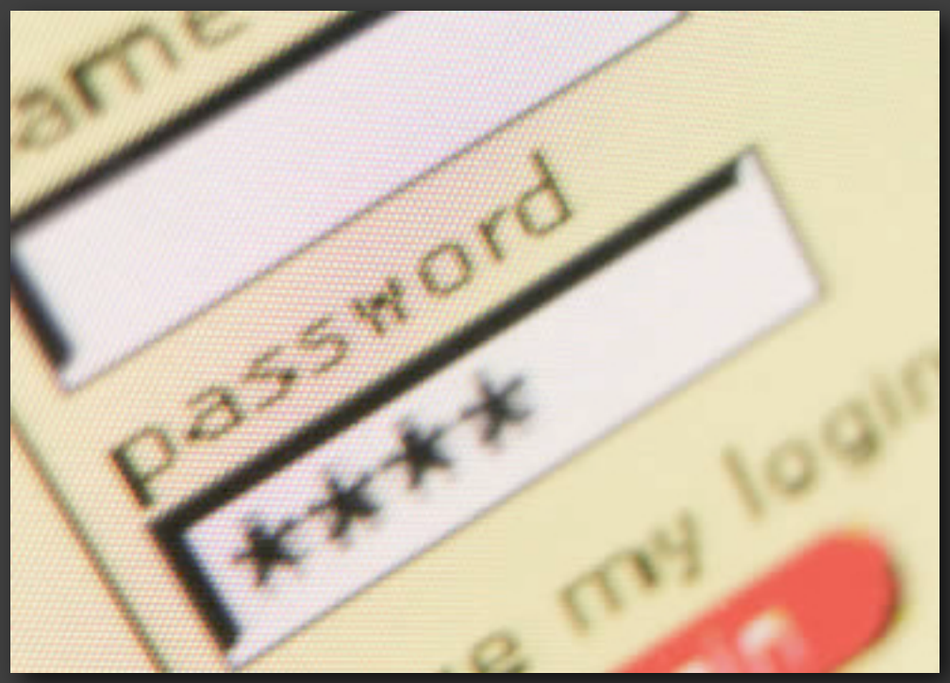
http://dnscrypt.org/

USE BETTER PASSWORDS

USE MORE PASSWORDS

SlashGear 101: Basic Password Security

"The simplest way to keep yourself secure on the internet is to use different passwords on each 'secure' site you interact with."

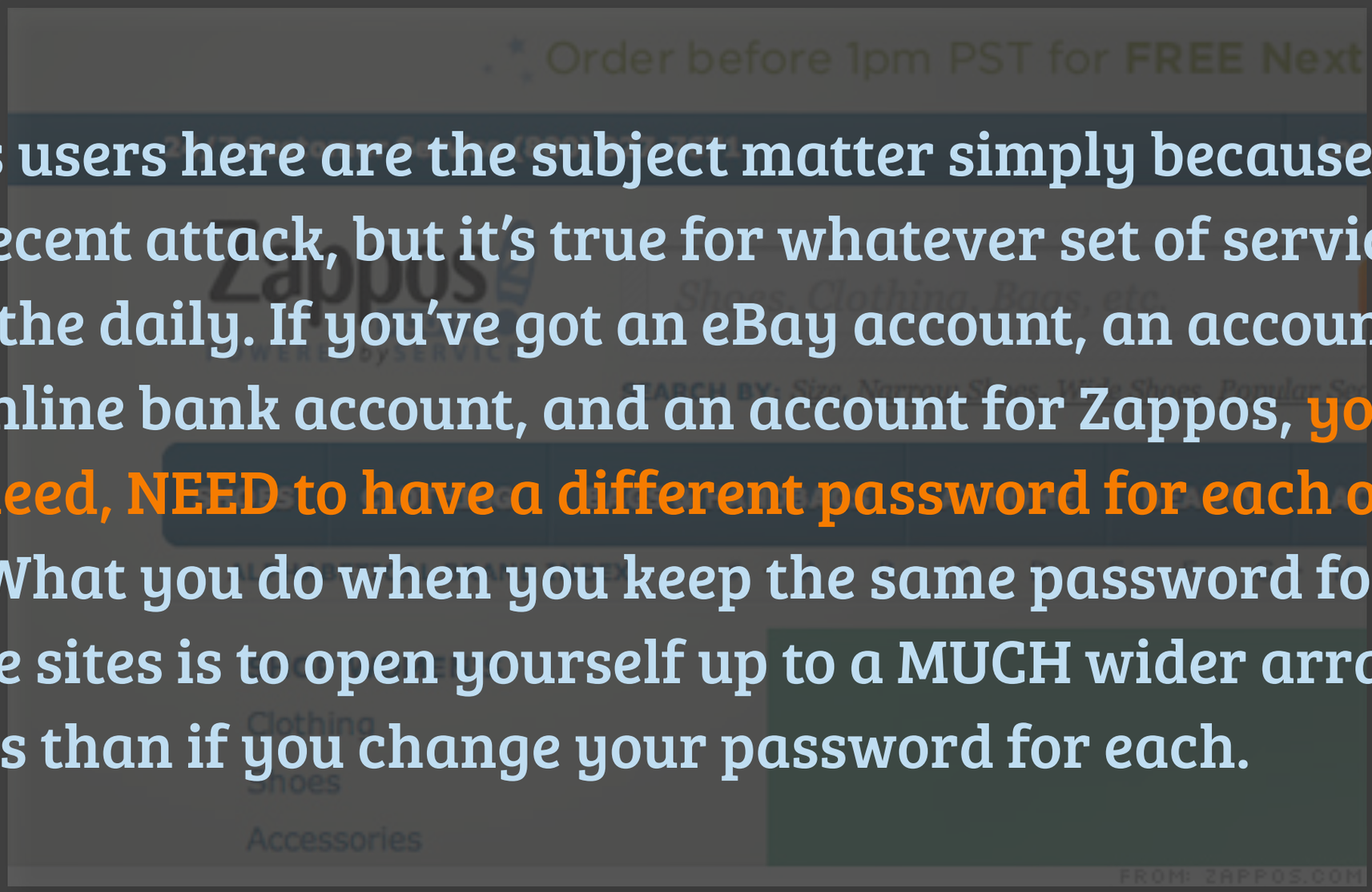


http://www.slashgear.com/slashgear-101-basic-password-security-16209438

Zappos hacked, 24 million accounts

http://money.cnn.com/2012/01/16/technology/zappos_hack/index.htm

Zappos hacked, 24 million accounts



Zappos users here are the subject matter simply because it's the most recent attack, but it's true for whatever set of services you use on the daily. If you've got an eBay account, an account for your online bank account, and an account for Zappos, you need, need, NEED to have a different password for each of them. What you do when you keep the same password for each of these sites is to open yourself up to a MUCH wider array of hackers than if you change your password for each.

http://money.cnn.com/2012/01/16/technology/zappos_hack/index.htm

FORGET YOUR PASSWORDS

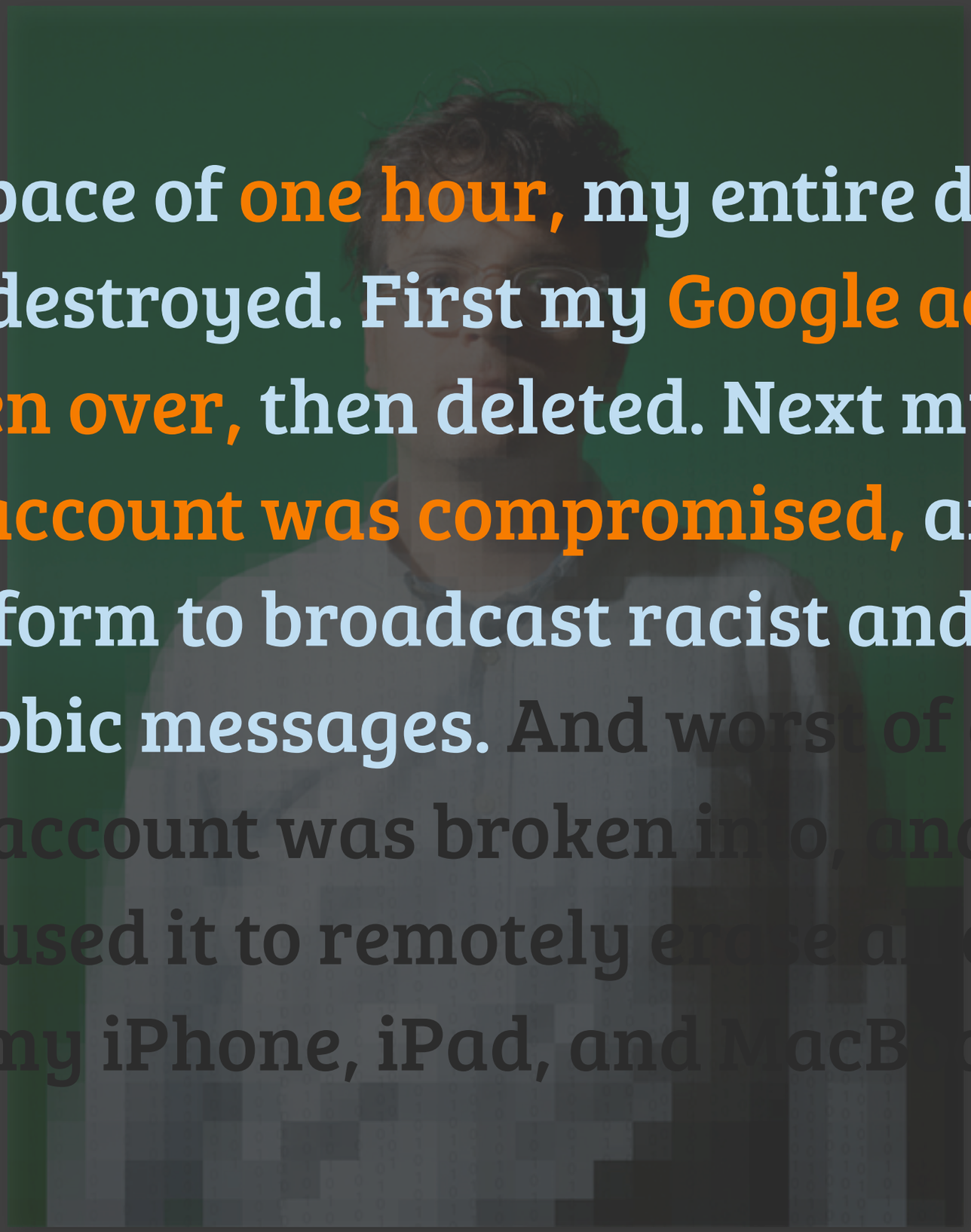
NOT

DID YOU FORGET YOUR PASSWORD?

WIRED

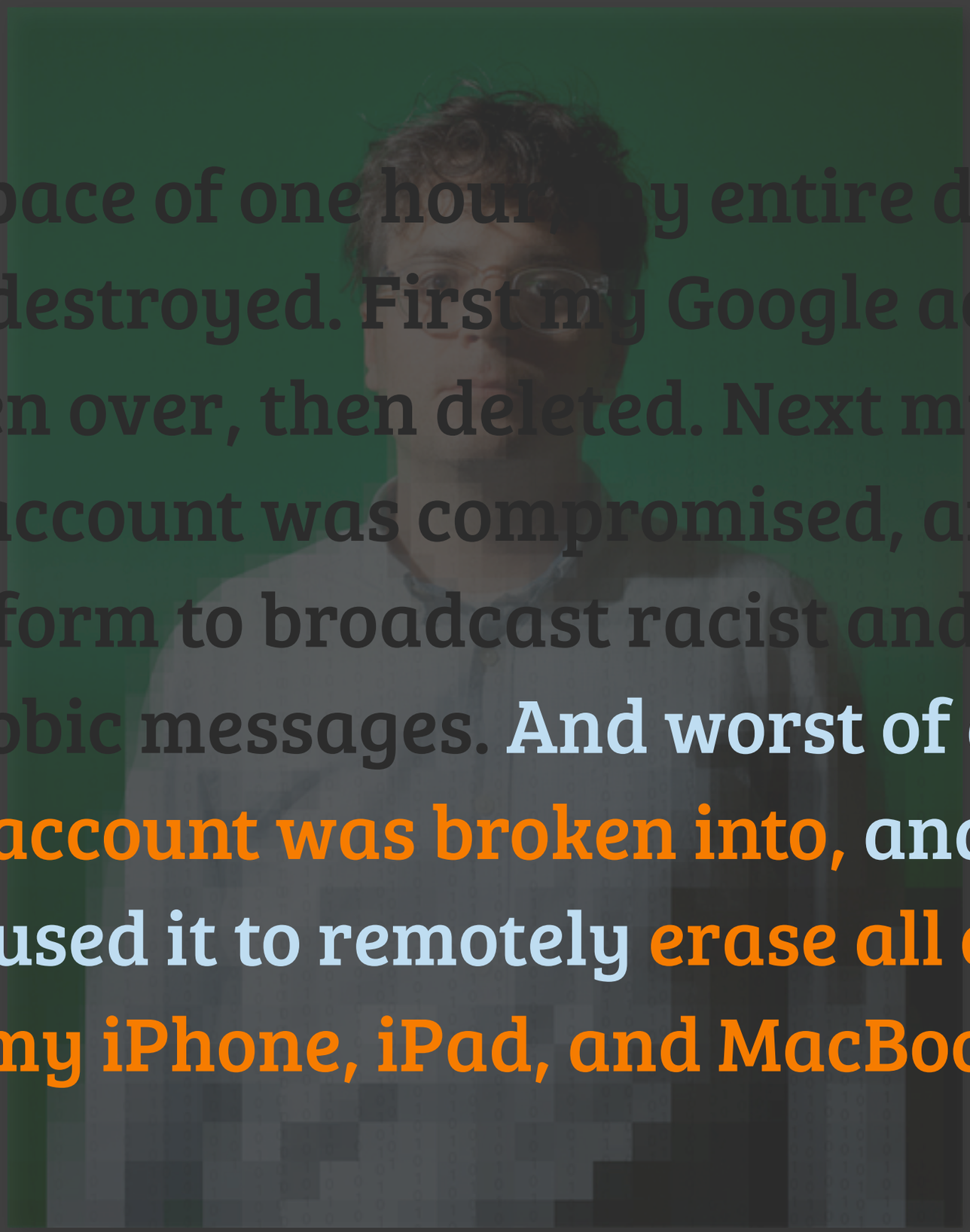
Mat Honan

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/



"In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook."

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/



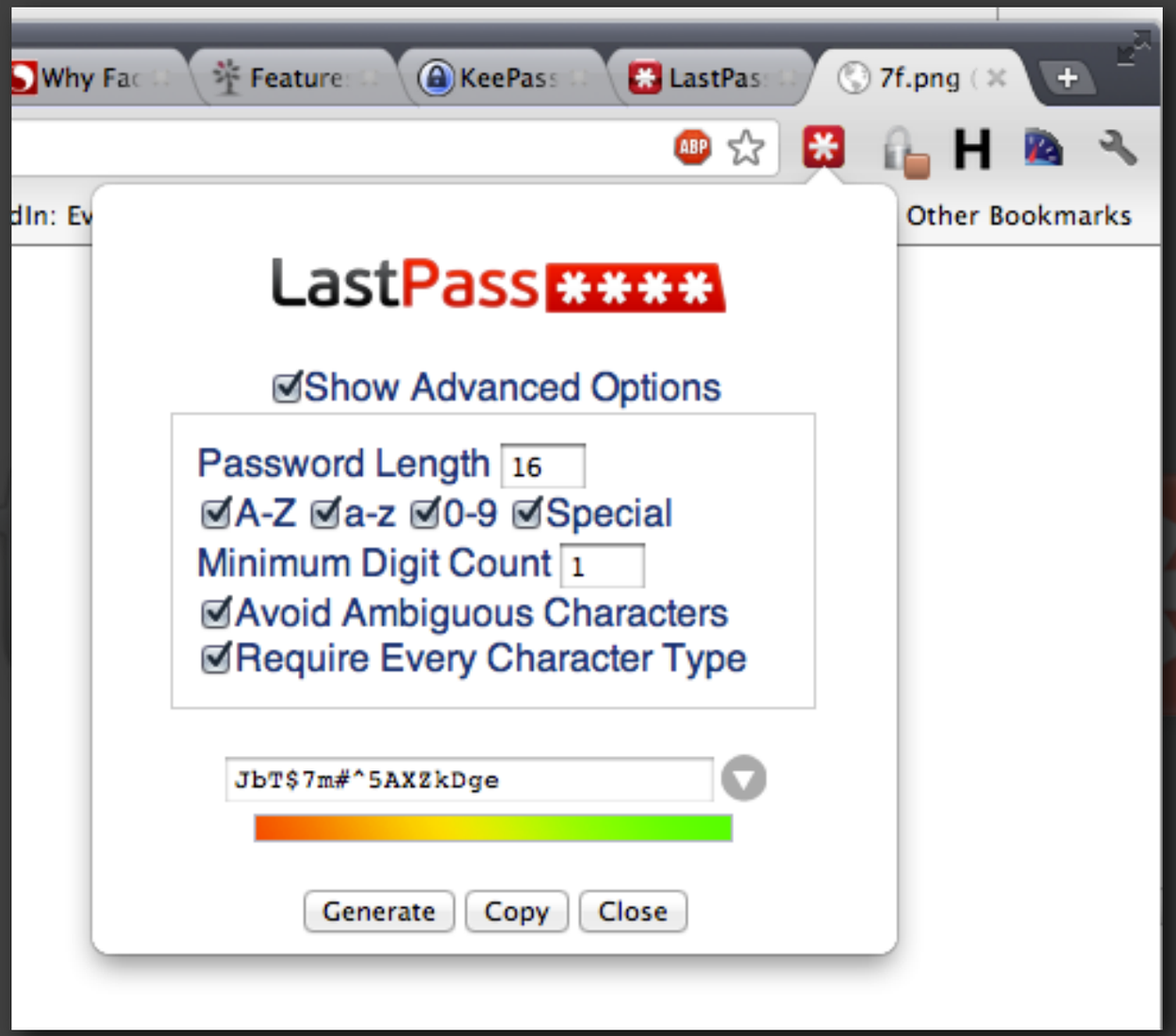
“In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.”

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

FORGET YOUR PASSWORDS

LastPass ****

https://lastpass.com


Why Fac
Feature
KeePass
LastPas
7f.png
dIn: Ev
Other Bookmarks
LastPass ****
Show Advanced Options
Password Length 16
A-Z a-z 0-9 Special
Minimum Digit Count 1
Avoid Ambiguous Characters
Require Every Character Type
JbT$7m#^5AXZkDge
Generate
Copy
Close

9Z!de*NM2y7%yZwt

wZx7CC@utHyVD@5K

cP$arcQTkt2Fhntu

#8cET!pDqDXq9HcV

9Z!de*NM2y7%yZwt

Not a perfect method, trusting a 3rd party

wZx7CC@utHyVD@5K

cP$arcQTkt2Fhntu

#8cET!pDqDXq9HcV

9Z!de*NM2y7%yZwt

Not a perfect method, trusting a 3rd party

wZx7CC@utHyVD@5K

Works, but looking for a more secure way

cP$arcQTkt2Fhntu

#8cET!pDqDXq9HcV

9Z!de*NM2y7%yZwt

Not a perfect method, trusting a 3rd party

wZx7CC@utHyVD@5K

Works, but looking for a more secure way

cP$arcQTkt2Fhntu

Ideally an Open Source option

#8cET!pDqDXq9HcV

SEARCH MORE SECURELY

Take a deep breath. You're safe here.

Click here to learn how Ixquick protects you from government surveillance.

https://ixquick.de/

No PRISM. No Surveillance. No Government Back Doors. You Have our Word on it.

Giant US government Internet spying scandal revealed

The Washington Post and The Guardian have revealed a US government mass Internet surveillance program code-named "PRISM". They report that the NSA and the FBI have been tapping directly into the servers of nine US service providers, including Facebook, Microsoft, Google, Apple, Yahoo, YouTube, AOL and Skype, and began this surveillance program at least seven years ago. (clarifying slides)

These revelations are shaking up an international debate.

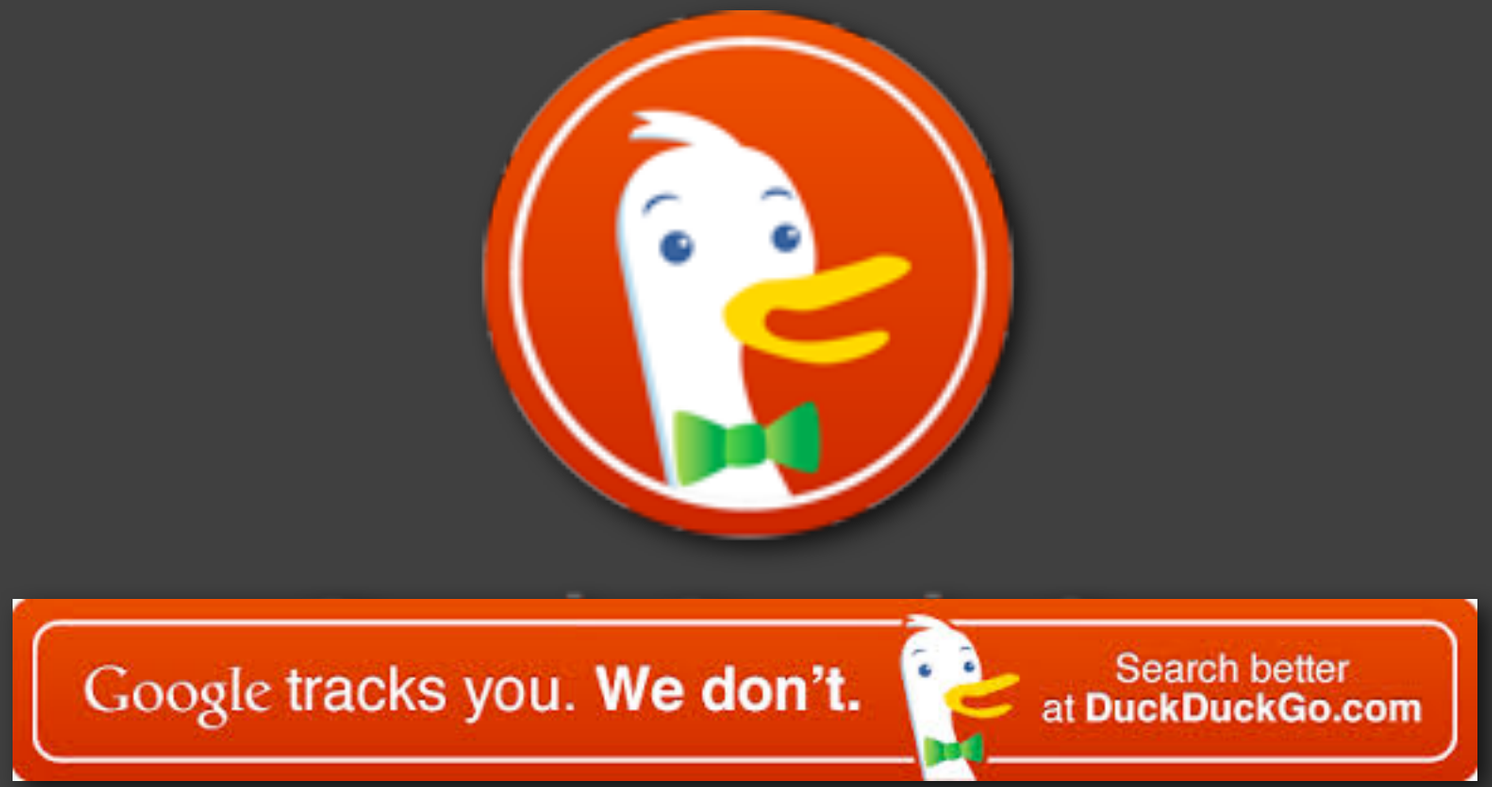
Ixquick has always been very outspoken when it comes to protecting people's Privacy and civil liberties. So it won't surprise you that we are a strong opponent of overreaching, unaccountable spy programs like PRISM. In the past, even government surveillance programs that were begun with good intentions have become tools for abuse, for example tracking civil rights and anti-war protesters.

Programs like PRISM undermine our Privacy, disrupt faith in governments, and are a danger to the free Internet.

Ixquick and its sister search engine **StartPage** have in their 14-year history never provided a single byte of user data to the US government, or any other government or agency. Not under PRISM, nor under any other program in the US, nor under any program anywhere in the world. We are not like Yahoo, Facebook, Google, Apple, Skype, or the other US companies who got caught up in the web of PRISM surveillance.

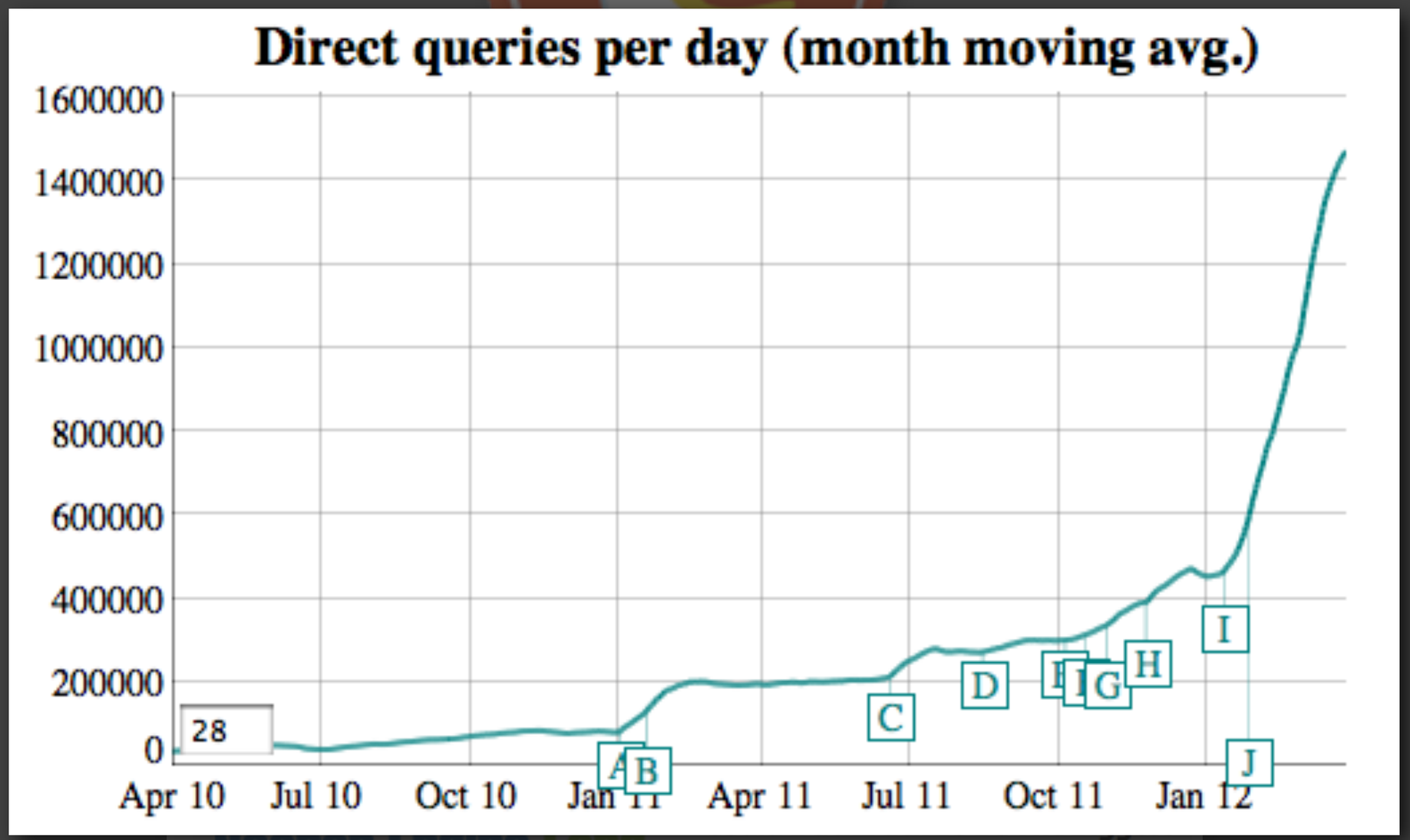
Click here to learn how Ixquick protects you from government surveillance.

https://ixquick.de/



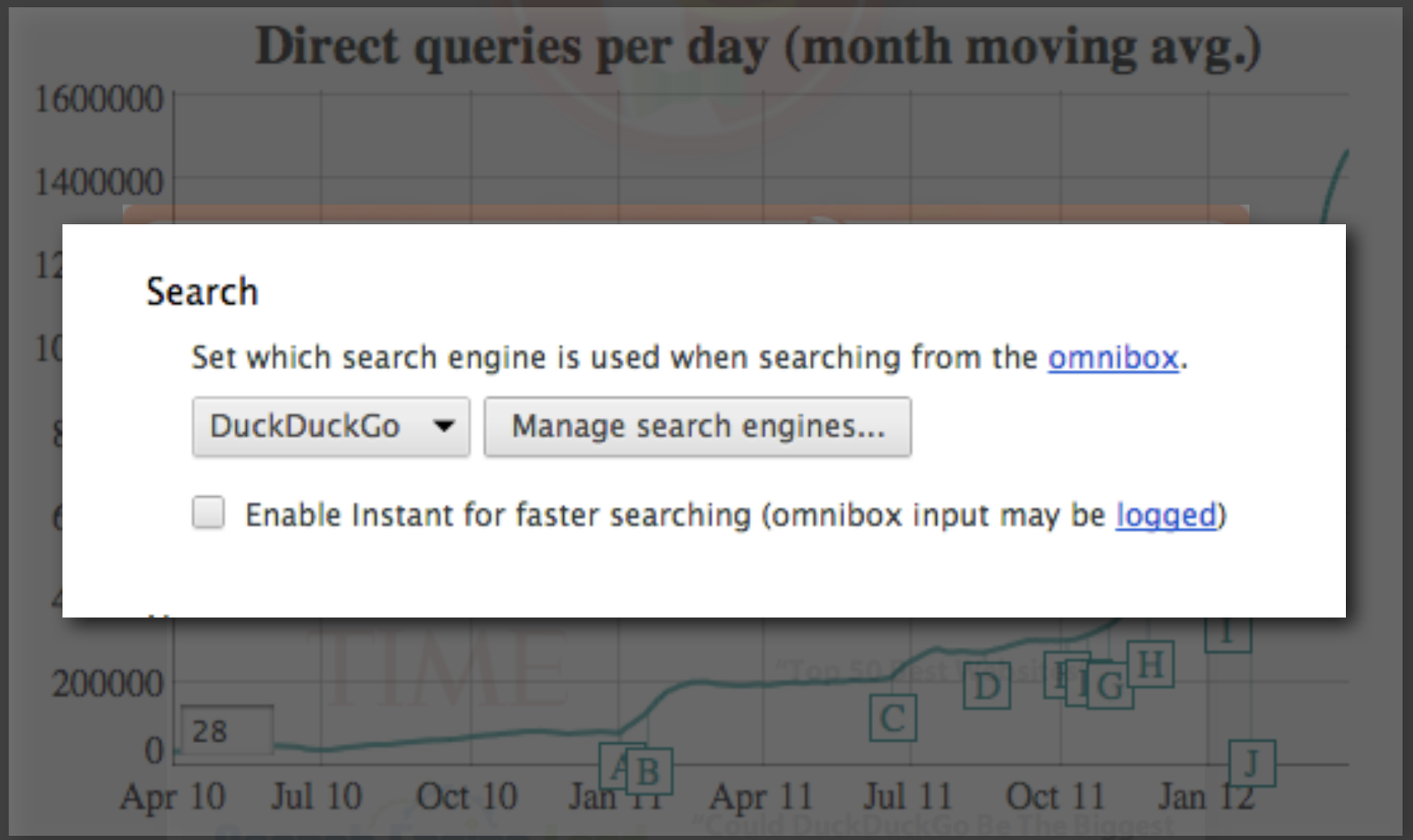
Search anonymously. Find instantly.

https://duckduckgo.com



Search anonymously. Find instantly.

https://duckduckgo.com



Search

Set which search engine is used when searching from the omnibox.

DuckDuckGo | Manage search engines...

Enable Instant for faster searching (omnibox input may be logged)

Search anonymously. Find instantly.

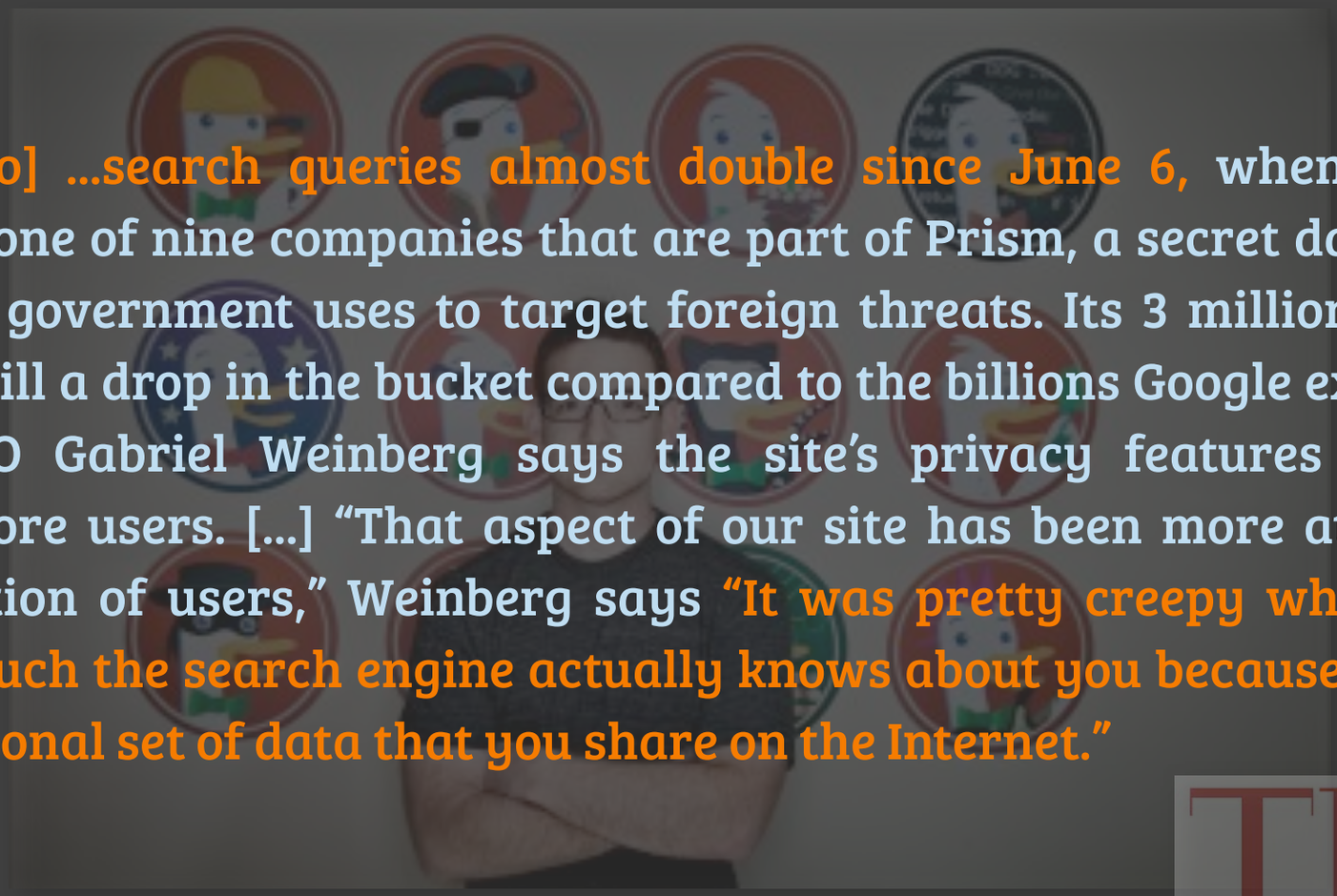
https://duckduckgo.com

The Anonymous Internet: Privacy Tools Grow in Popularity Following NSA Revelations

TIME

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

The Anonymous Internet: Privacy Tools Grow in Popularity Following NSA Revelations



"[DuckDuckGo] ...search queries almost double since June 6, when Google was identified as one of nine companies that are part of Prism, a secret data-gathering program the government uses to target foreign threats. Its 3 million daily direct searches is still a drop in the bucket compared to the billions Google executes every day, but CEO Gabriel Weinberg says the site's privacy features are steadily attracting more users. [...] "That aspect of our site has been more attractive to a growing portion of users," Weinberg says "It was pretty creepy when you think about how much the search engine actually knows about you because it's arguably the most personal set of data that you share on the Internet."

TIME

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

The Anonymous Internet: Privacy Tools Grow in Popularity Following NSA Revelations

"Kobeissi points out that even if these tools help with anonymisation, they can't completely deter dedicated government surveillance. "The real solution is not just telling people to depend on these tools. The real solution is to get an honest political discussion going on to limit or get rid of these surveillance tactics."

TIME

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

“A peer to peer (P2P), distributed, anonymous search engine anyone can run and contribute to”

"[...] we cannot rely on a few large companies, and compromise our privacy in the process," says Michael Christen, YaCy's project leader. "YaCy's free search is the vital link between free users and free information. YaCy hands control over search back to us, the users."

http://yacy.net

http://www.theregister.co.uk/2011/11/29/yacy_google_open_source_engine

PAY DIFFERENTLY

http://bitcoin.org

- a P2P digital currency
- a protocol and software that enables instant peer-to-peer transactions and worldwide payments
- it is open source under the MIT license

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

- a P2P digital currency
- a protocol and software that enables instant peer-to-peer transactions and worldwide payments
- it is open source under the MIT license

- has burst into the mainstream consciousness this year
- now being accepted everywhere from New York bars to dating website OKCupid

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

- a P2P digital currency
- a protocol and software that enables instant peer-to-peer transactions and worldwide payments
- is open source under the MIT license

Buyer beware though: Bitcoin values are extremely volatile

- has burst into the mainstream consciousness this year
- now being accepted everywhere from New York bars to dating website OKCupid

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

ency

tware that enables instant peer-to-

and worldwide payments

nder the MIT licens

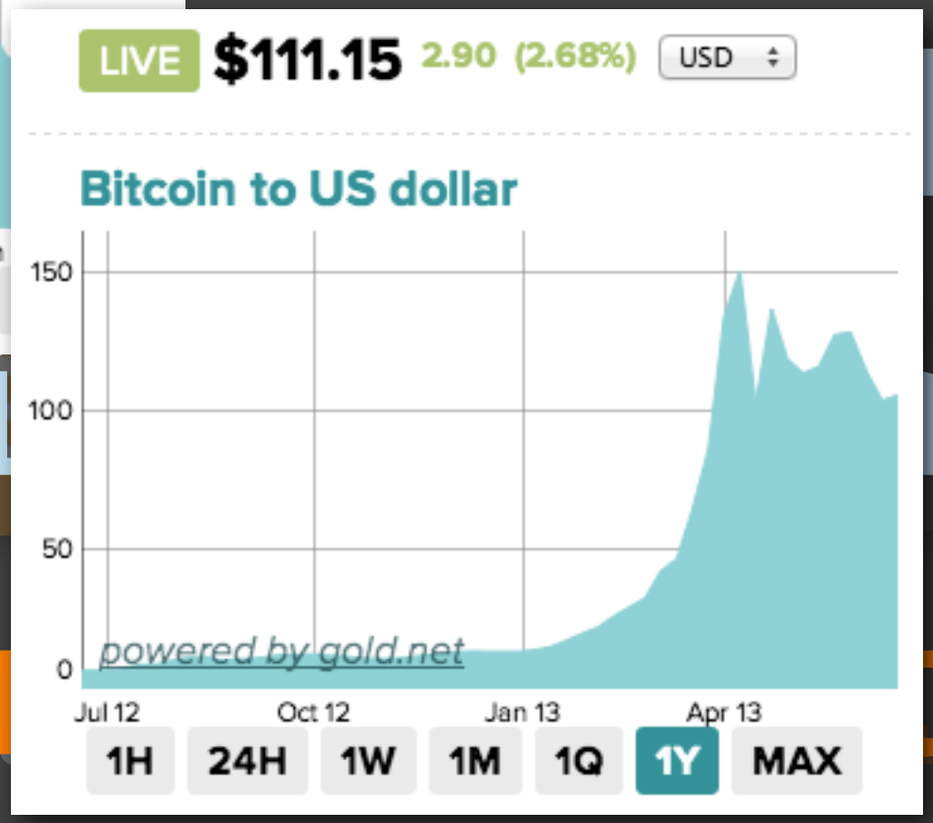
eware though:

Bitcoin values are extremely volatile

- has burst into the mainstream consciousness this year
- now being accepted everywhere from New York bars to dating website OKCupid

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/



ency

tware that enables instant peer-to-

and worldwide payments

hough:

re

Bitcoi

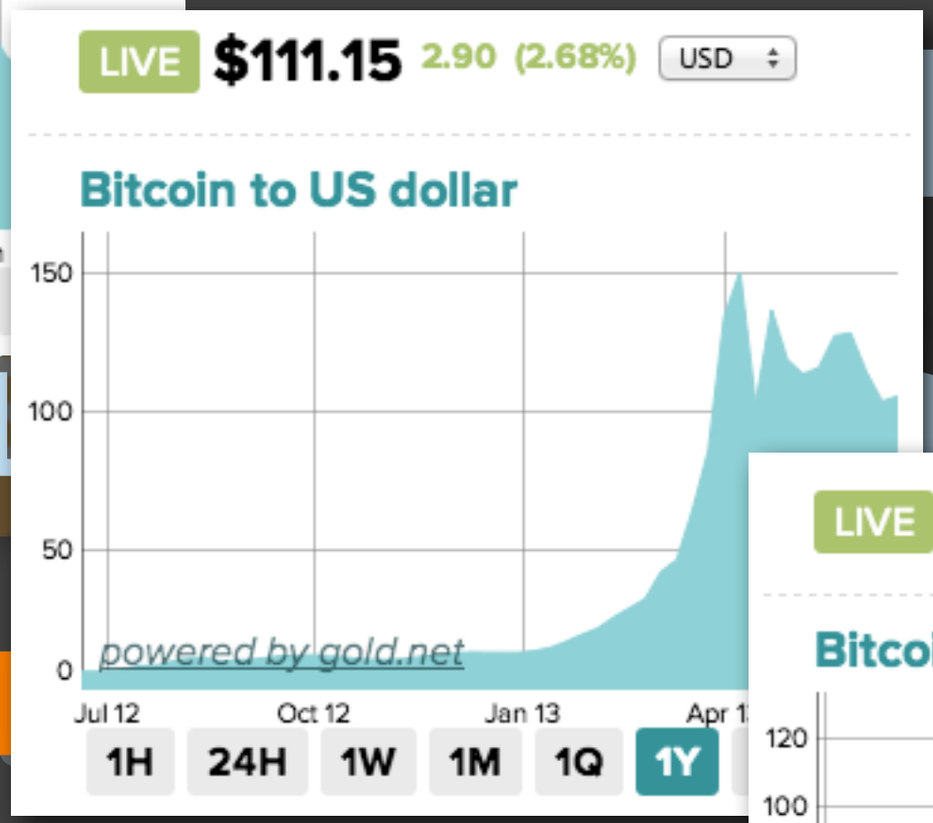
extre

tile

- has burst into [illegible] business this year
- now being accepted everywhere from New York bars to dating website OKCupid

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/



Bitcoi

extre

- has burst int
- now being accepted everywhere fr
  dating website OKCupid

ency

tware that enables instant peer-to-

and worldwide payments

hough:

re

https://bitcoin.org/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

SHARE MORE SECURELY

https://spideroak.com/

Provides similar functionality to DropBox and Google Drive...

BUT is a "zero-knowledge" client, meaning the company can't see the content of user files, which are automatically encrypted

Taking your data into your own hands has its pros/cons:
SpiderOak can't retrieve your password for you if you forget it

https://spideroak.com/
http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

Provides similar functionality to DropBox and Google Drive...

BUT is a "zero-knowledge" client, meaning the company can't see the content of user files, which are automatically encrypted

Taking your data into your own hands has its pros/cons:
SpiderOak can't retrieve your password for you if you forget it

https://spideroak.com/
http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

Provides similar functionality to DropBox and Google Drive...

BUT is a "zero-knowledge" client, meaning the company can't see the content of user files, which are automatically encrypted

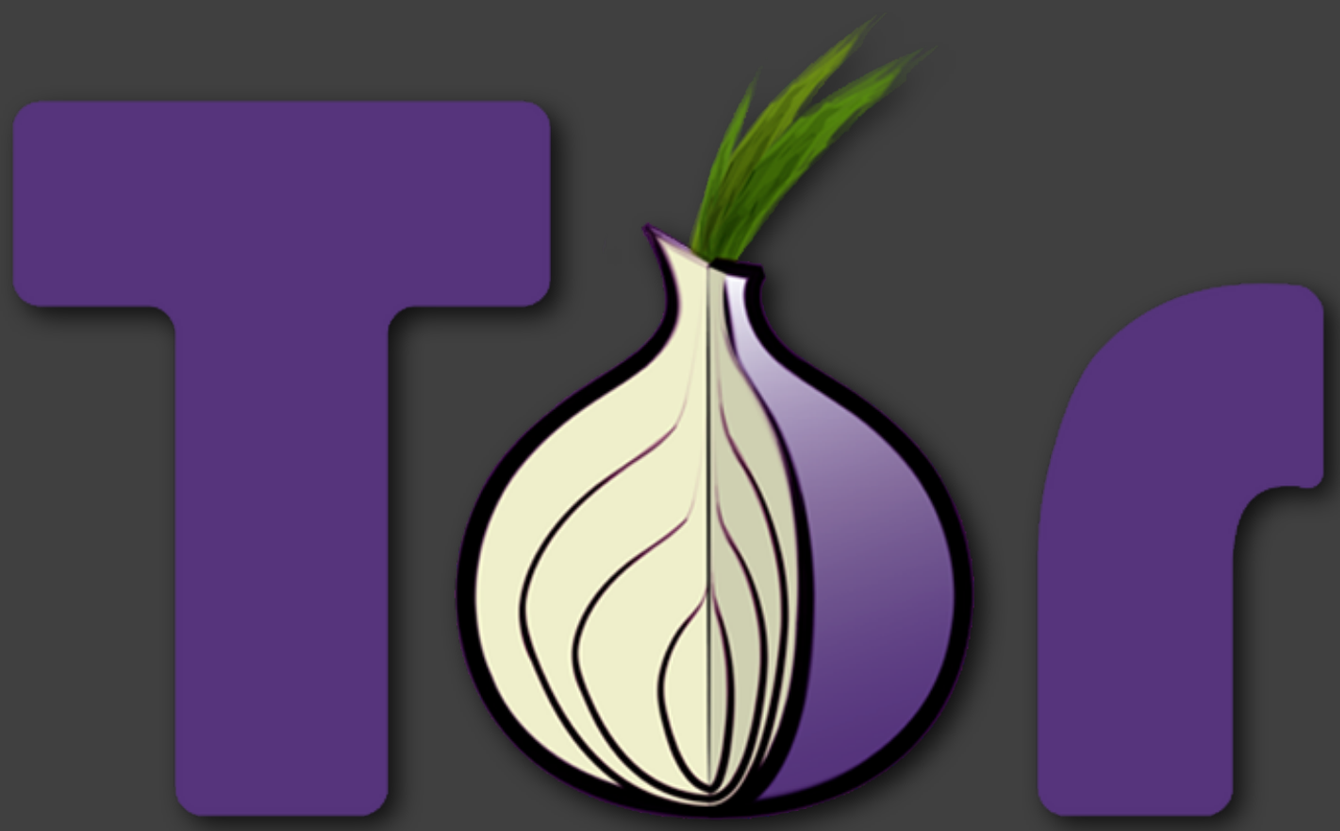
Taking your data into your own hands has its pros/cons:

SpiderOak can't retrieve your password for you if you forget it

https://spideroak.com/

http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

USE OPEN SOURCE TOOLS TO PROTECT YOURSELF



https://torproject.org

Originally called The Onion Router, and started out as a US Naval project

Protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world

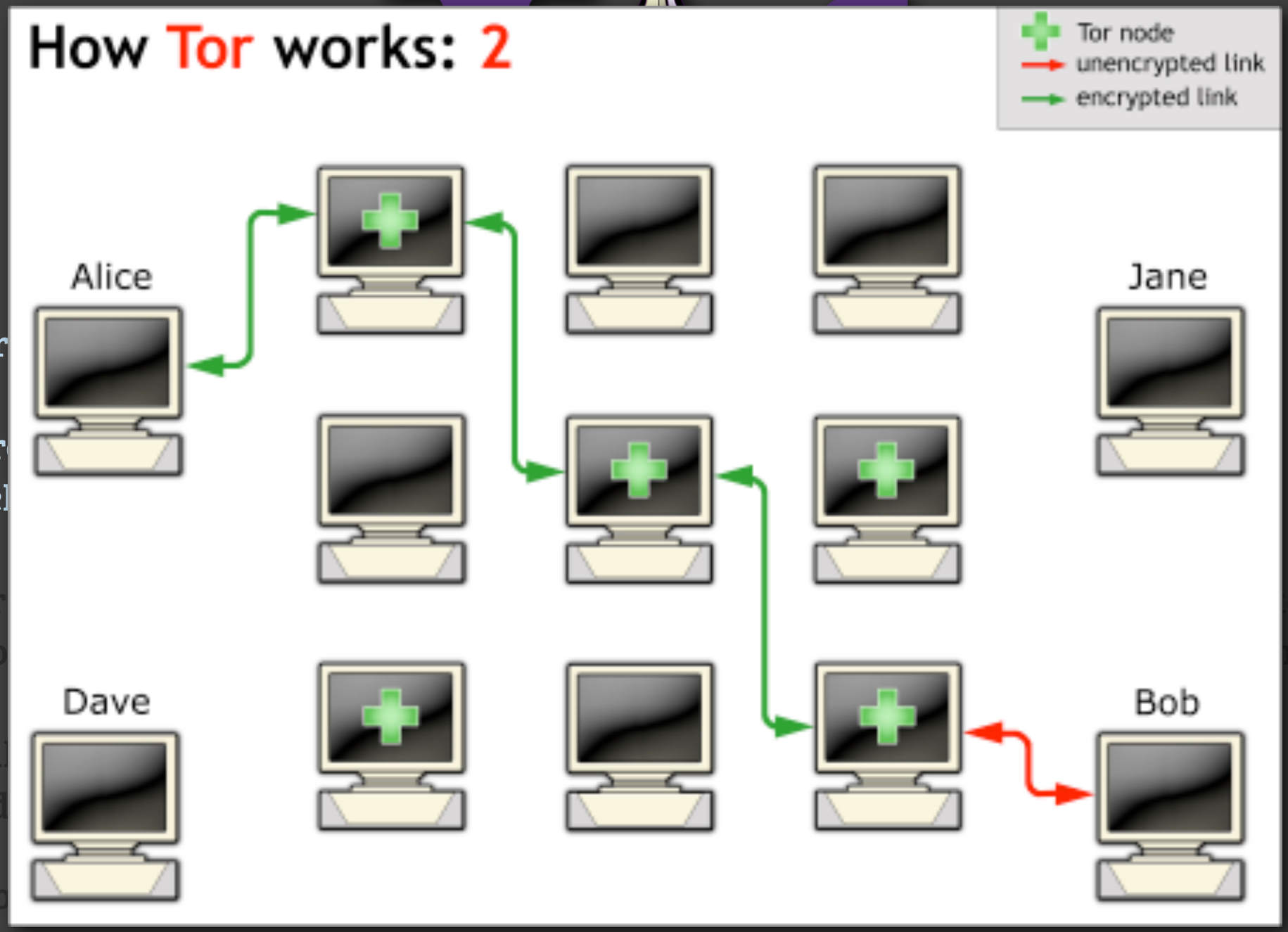
Prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location

Allows users to surf the Internet (...almost...) anonymously by making IP addresses difficult to trace

Downloads increase between 20% and 30% following the NSA news

It has been downloaded 36 million times in the past year and has more than half a million daily users

https://torproject.org



It has been downloaded 36 million times in the past year and has more than half a million daily users

Originally called The Onion Router, and started out as a US Naval project

Protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world

Prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location

Allows users to surf the Internet (...almost...) anonymously by making IP addresses difficult to trace

Downloads increase between 20% and 30% following the NSA news

It has been downloaded 36 million times in the past year and has more than half a million daily users

https://torproject.org

Originally called The Onion Router, and started out as a US Naval project

Protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world

Prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location

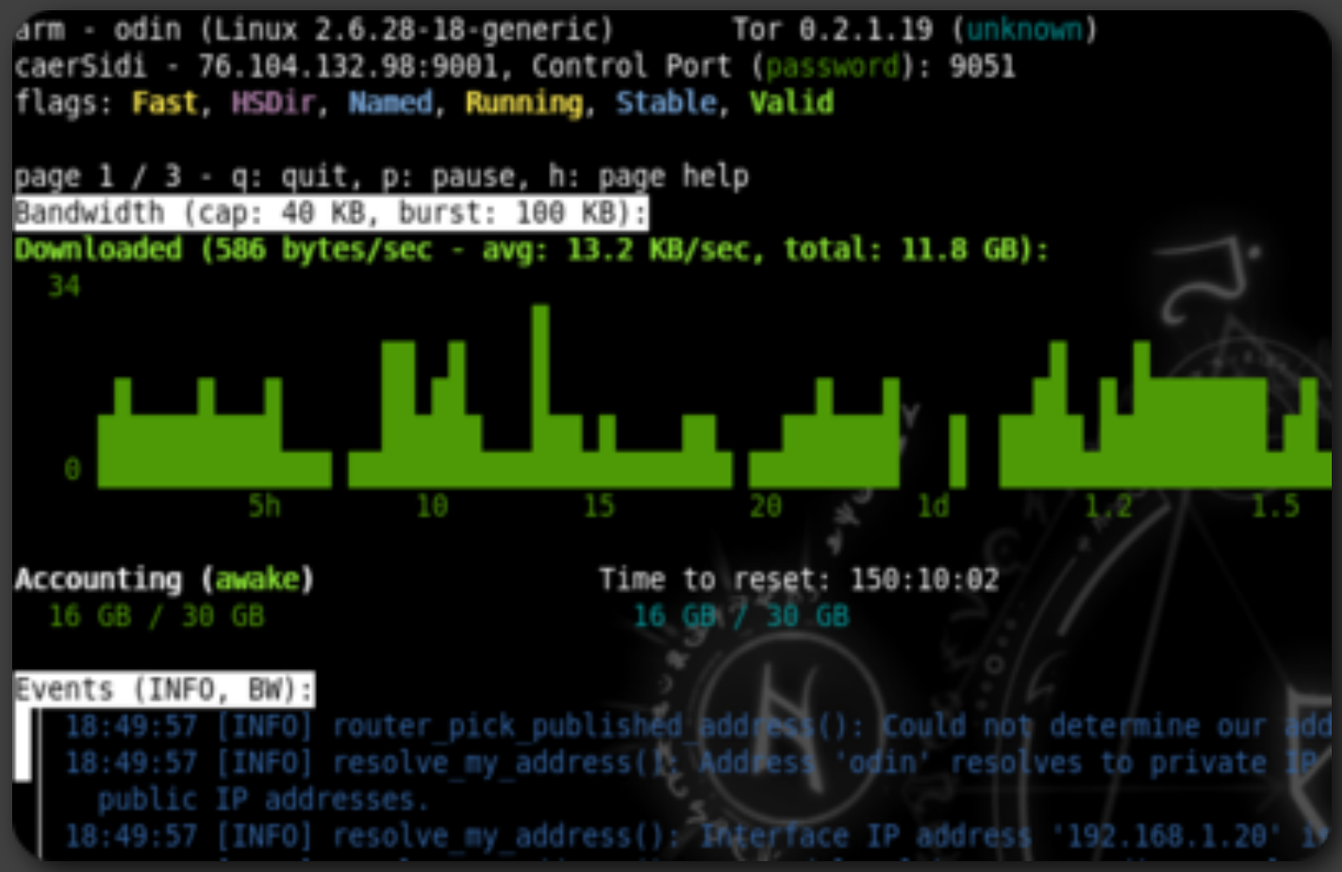
Allows users to surf the Internet (...almost...) anonymously by making IP addresses difficult to trace

Downloads increase between 20% and 30% following the NSA news

It has been downloaded 36 million times in the past year and has more than half a million daily users

The Tor Browser Bundle lets you use Tor on Windows, Mac OS X or Linux without installing any software.

https://www.torproject.org/projects/torbrowser.html.en



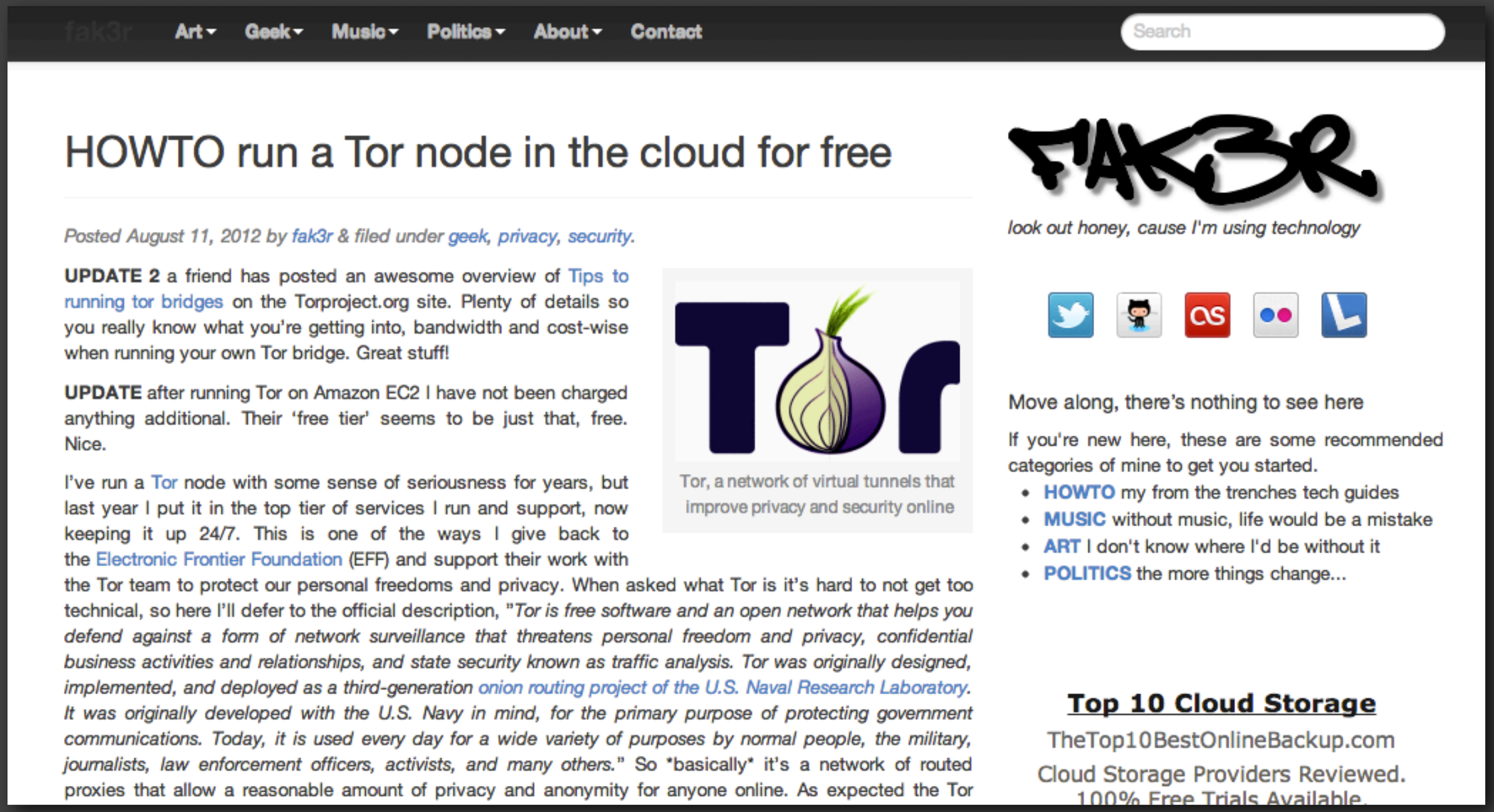
Install Tor on a server
to contribute to the network's robustness, and connect yourself

https://torproject.org

Tor Cloud

- a user-friendly way of deploying Tor bridges to help users access an uncensored Internet
- runs on a Amazon EC2 micro cloud computing platform
- Amazon has introduced a free usage tier for a year

https://cloud.torproject.org

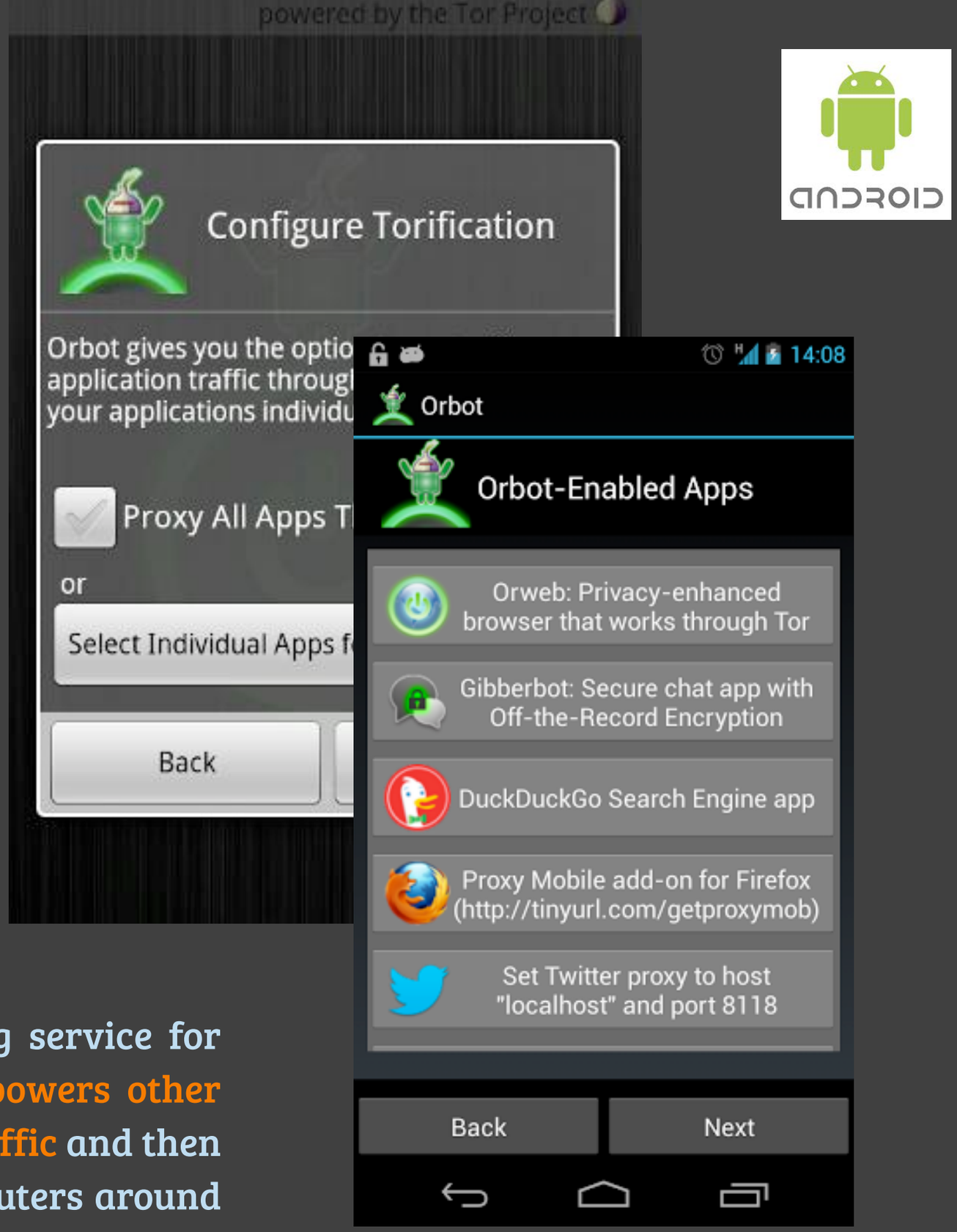


fak3r.com post: HOWTO run a tor node in the cloud for free

http://fak3r.com/2012/08/11/howto-run-a-tor-node-in-the-cloud-for-free/

DON’T FORGET ABOUT MOBILE COMMUNICATIONS (THE NSA ISN’T)

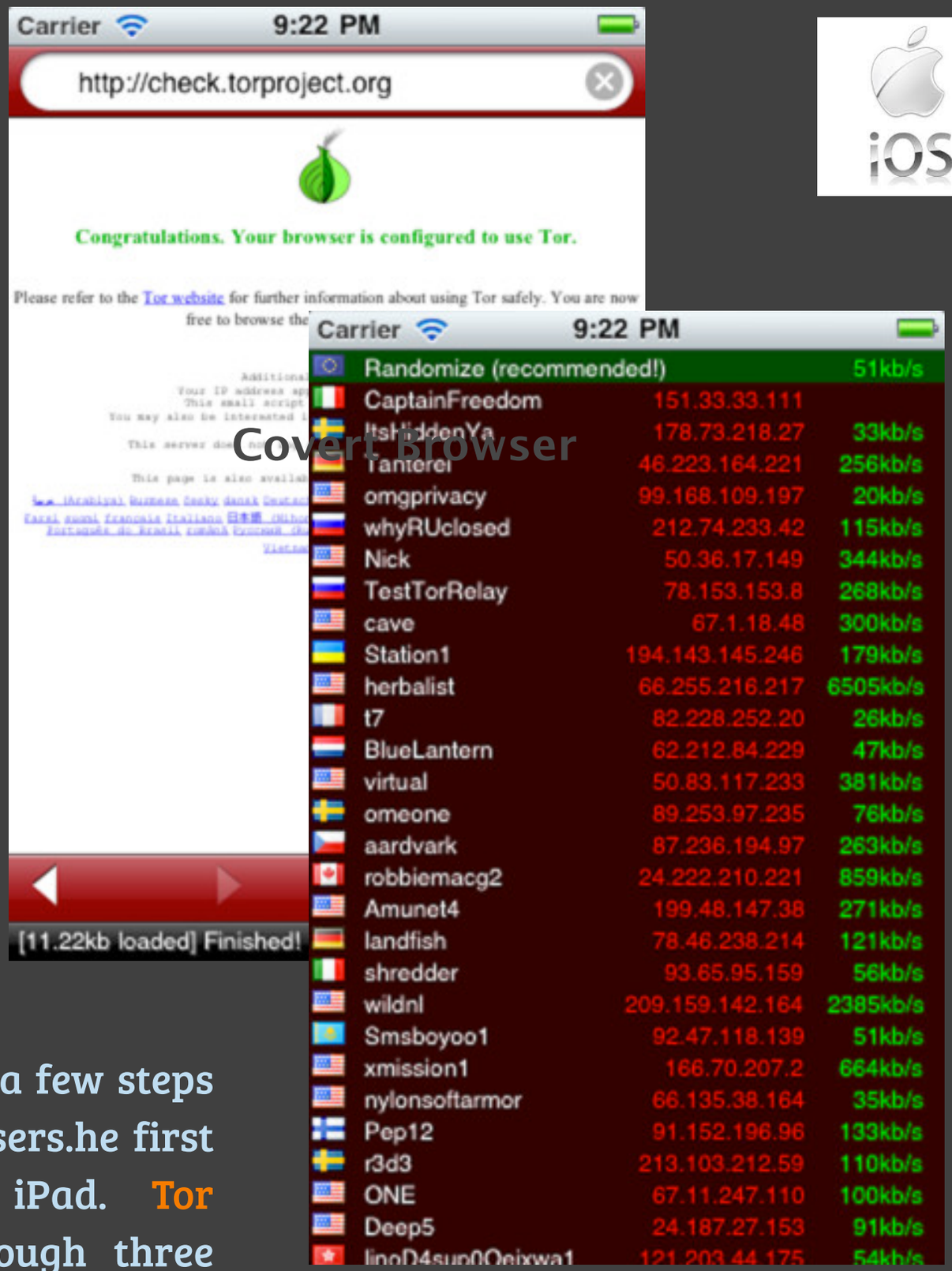
Orbot



"The official version of the Tor onion routing service for Android. Orbot is a free proxy app that empowers other apps to use [...] Tor to encrypt your Internet traffic and then hides it by bouncing through a series of computers around the world. Any installed app can use Tor if it has a proxy feature"

https://guardianproject.info/apps/orbot/

Covert Browser



"True anonymity on the mobile Web just came a few steps closer for tens of millions more smartphone users.he first official implementation of Tor for iPhone and iPad. Tor triple-encrypts data and then routes it through three different computers around the world, each one removing only one layer of encryption."

https://itunes.apple.com/us/app/covert-browser/id477438328?mt=8

WHISPERSYSTEMS

“Whipsersystems - Secure your communication with our mobile applications. It's that simple. Encrypted Communication And Storage [...] easy to use tools for secure mobile communication and secure mobile storage. Open Source Software”

https://whispersystems.org/

Gibberbot

"Free, secure, unlimited messaging with your friends over Facebook Chat, Google Chat & Jabber Works with Android, iPhone, Mac, Linux or PC. [...] iPhone with ChatSecure, Mac with Adium, Linux with Jitsi, Windows with Pidgin"

https://guardianproject.info/apps/gibber/

Crytocat

https://crypto.cat/

Crytocat

Encrypted IM can be easy and accessible

Cryptocat is an open source experiment

Works right in your browser

Goal is to provide the easiest, most accessible way to chat while maintaining your privacy online

It's useful for everyone

Friends use Cryptocat to talk without revealing messages to a third party

Activists use Cryptocat to keep private matters private

Journalists use Cryptocat to keep their stories and research confidential

Cryptocat is not a magic bullet. You should never trust any piece of software with your life, and Cryptocat is no exception

https://crypto.cat/

Crytocat

Encrypted IM can be easy and accessible

Cryptocat is an open source experiment

Works right in your browser

Goal is to provide the easiest, most accessible way to chat while maintaining your privacy online

It's useful for everyone

Friends use Cryptocat to talk without revealing messages to a third party

Activists use Cryptocat to keep private matters private

Journalists use Cryptocat to keep their stories and research confidential

Cryptocat is not a magic bullet. You should never trust any piece of software with your life, and Cryptocat is no exception

https://crypto.cat/

Crytocat

Encrypted IM can be easy

Cryptocat is an open sou

Works right in your brow

Goal is to provide the eas ning your privacy online

It's useful for everyone

Friends use Cryptocat to y

Activists use Cryptocat t

Journalists use Cryptoca l

Cryptocat is not r trust any piece of software with your life, and Cryptocat is no exception

https://crypto.cat/

Who has your metadata when you use Cryptocat?	Cryptocat Server	Your ISP
Conversation name	**Yes**	**No**
Your nickname	**Yes**	**No**
Can see that you are connecting to Cryptocat	**Yes** (Sees a connecting IP)	**Yes** (Except if using Tor)
Time messages were sent	**Yes**	**Yes**
Which nicknames you are messaging privately/ having file transfers with	**Yes**	**No**
Your IP address	**Yes** (Except if using Tor)	**Yes**
Contents of conversation	**No**	**No**
Contents of file transfers	**No**	**No**
Names of files transferred	**No**	**No**
Sizes of files transferred	**Yes** (Approximately)	**Possibly**
Types of files transferred	**Yes**	**No**
Public keys and fingerprints	**Yes**	**No**
Private keys	**No**	**No**

Crytocat

Encrypted IM can be easy and accessible

Cryptocat is an open source experiment

Works right in your browser

Goal is to provide the easiest, most accessible way to chat while maintaining your privacy online

It's useful for everyone

Friends use Cryptocat to talk without revealing messages to a third party

Activists use Cryptocat to keep private matters private

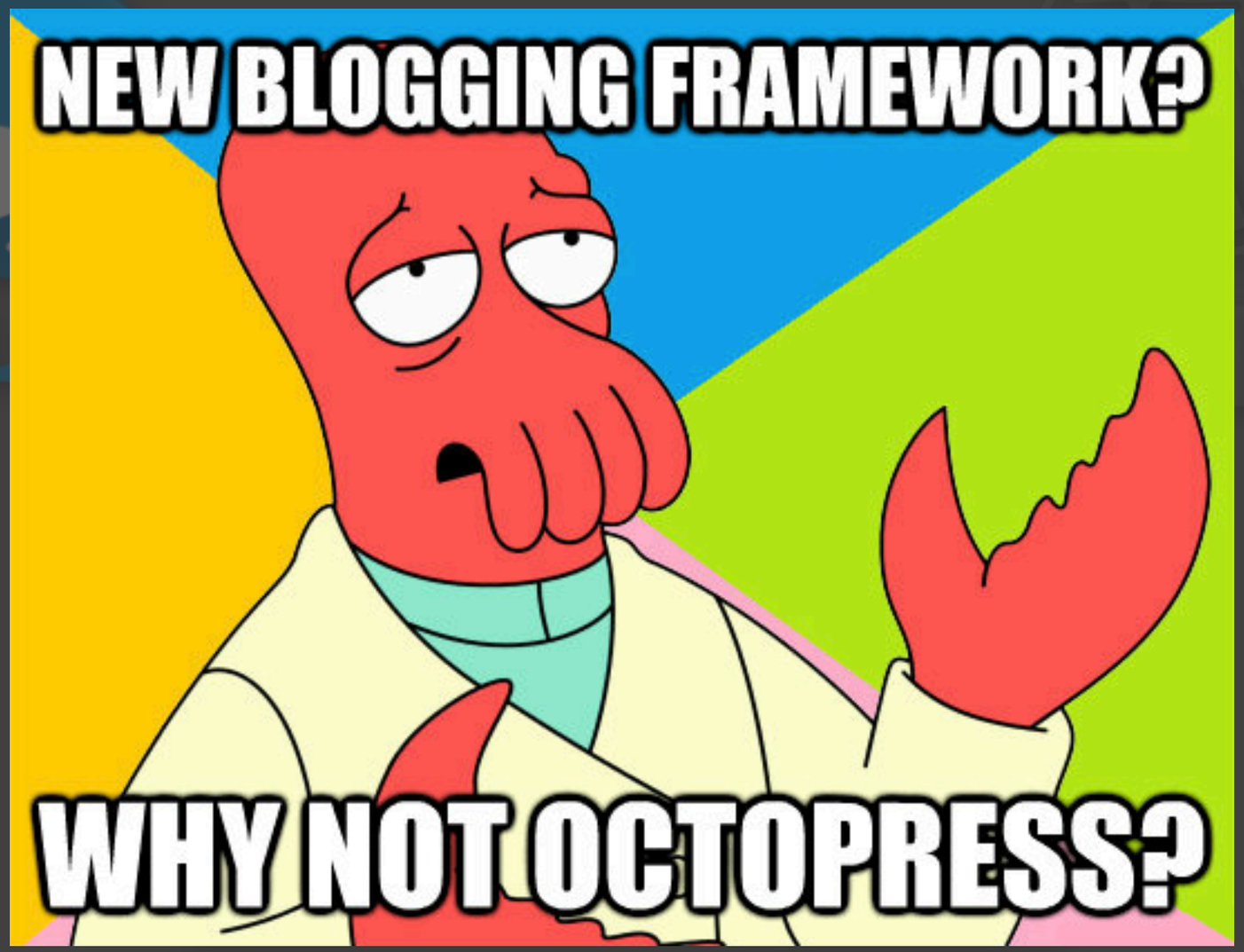
Journalists use Cryptocat to keep their stories and research confidential

Cryptocat is not a magic bullet. You should never trust any piece of software with your life, and Cryptocat is no exception

https://crypto.cat/

DIY, RUN YOUR OWN SERVICES,
INSTEAD OF USING OTHERS

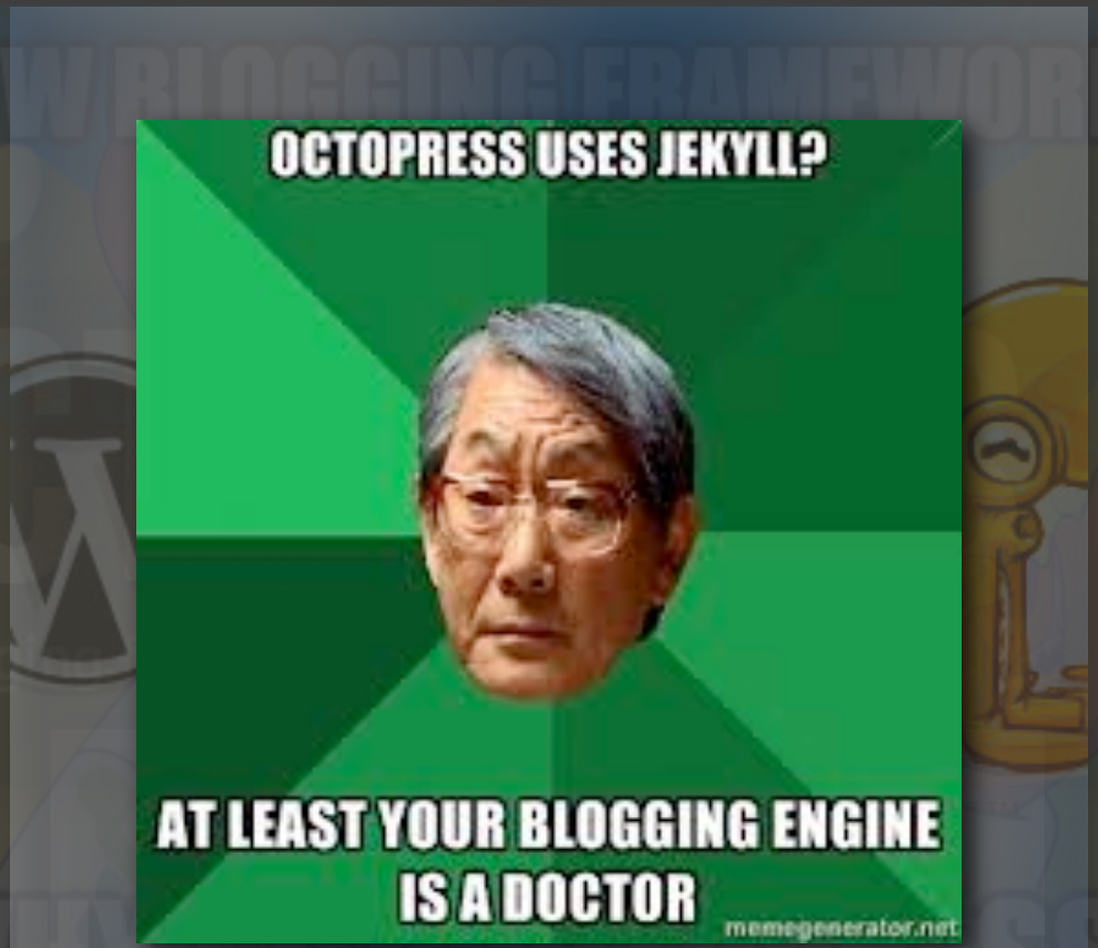
http://drupal.org
http://wordpress.org
http://joomla.org



http://octopress.com

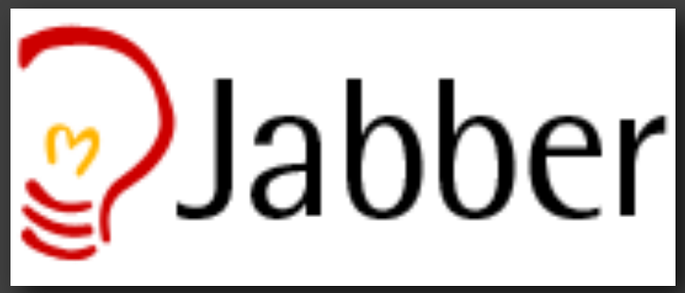
http://octopress.com

http://octopress.com


OCTOPRESS USES JEKYLL?
AT LEAST YOUR BLOGGING ENGINE IS A DOCTOR
memegenerator.net

http://jekyllrb.com

http://github.com



Open source, Jabber/XMPP instant messaging server, offers Off-the-Record (OTR) Messaging, more secure, SSL for encrypted communications, note that Google uses this same service for Google Talk

status.net™

Open source microblogging software (think Twitter), run your own host, keep your own information, and it powers Identi.ca

http://identi.ca
http://status.net/open-source

An open, distributed, federated, social network, mirrors functionality of Facebook, Google+, signup on an official server, or host your own and have full control over what you share

https://joindiaspora.com

lipsync.info

lipsync!

an open source, commandline service that securely syncronizes your data. Powered by rsync, OpenSSH, lsyncd and fak3r.

Think of it as a lightweight commandline version of Dr0pb0x that gives control back to you; the user and owner of the data.

Learn more »

Sync

Using realtime aspects of the operating system, lipsync's backend, lsyncd, ensures your files are synced immediately with the response you've come to expect from a *cough* closed source, proprietary solution. Once you have it working you can...

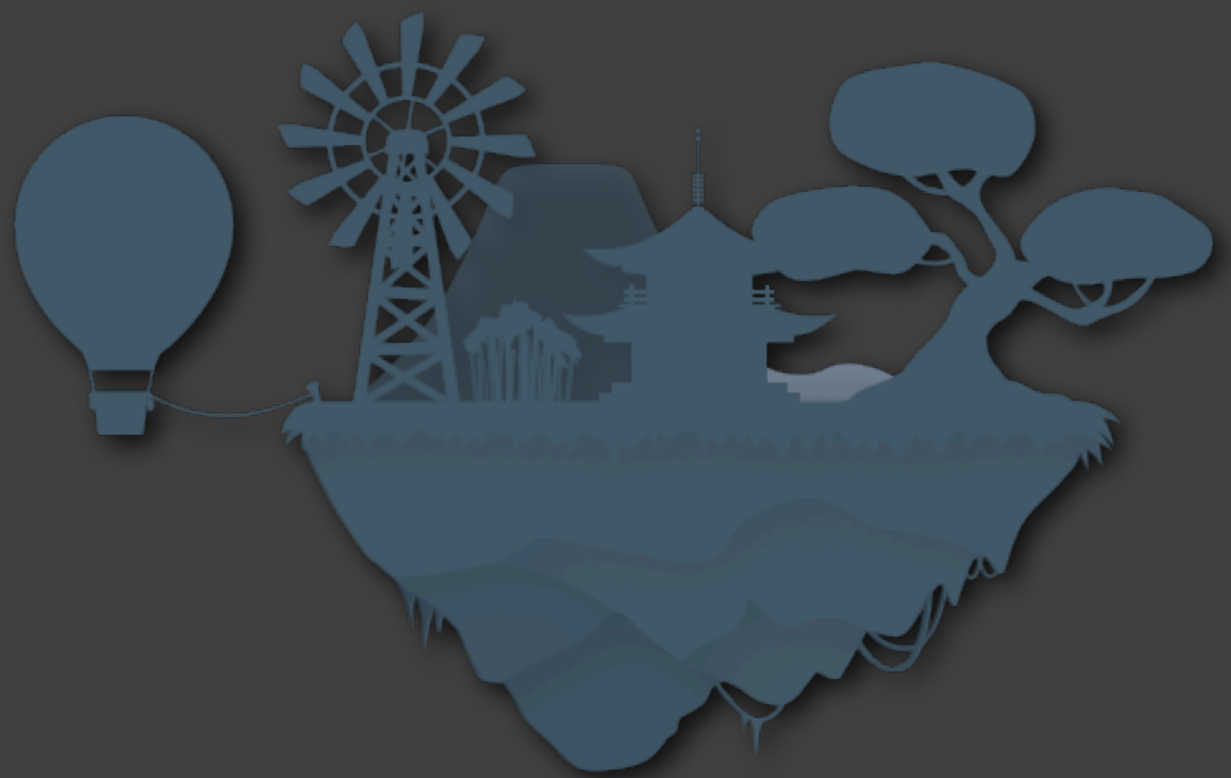
Extend

Since lipsync is open source, it's simple to add to and extend its functionality. What else would you want a sync'ing script to do for your files? Whatever it is, it's likely pretty simple to add to lipsync. Take a look at the code and then...

Get involved

Lipsync would be nothing without open source, and open source would be nothing without users. See something you want improved? Add it and share with the community, understand something better than others? Offer your expertise and help us make lipsync better!

A lightweight command line service that securely synchronizes your data http://lipsync.info



UNHOSTED.ORG

“...javascript based authentication, uses remoteStorage, a cross-origin data storage protocol separating application servers from data storage, your stuff on remote servers, but you still 'hold the keys'“

GET INVOLVED AND DEMAND CHANGE

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
Focusing public attention on emerging privacy and civil liberties issues

PrivacyMatters.com
Your Credit. Your Future.

EUROPEAN DIGITAL RIGHTS

FPF
FUTURE OF PRIVACY FORUM

ACLU
AMERICAN CIVIL LIBERTIES UNION
Protecting Civil Liberties in the Digital Age

PRIVACY INTERNATIONAL

PRC
Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

RECLAIM PRIVACY
.ORG

IN CONCLUSION...

Question HOW COMPANIES SAVE, STORE AND USE YOUR PERSONAL DATA

Question HOW COMPANIES SAVE, STORE AND USE YOUR PERSONAL DATA

Learn ABOUT ONLINE PRIVACY AND KNOW YOUR RIGHTS!

Question HOW COMPANIES SAVE, STORE AND USE YOUR PERSONAL DATA

Learn ABOUT ONLINE PRIVACY AND KNOW YOUR RIGHTS!

Share WHAT YOU DISCOVER, EDUCATE OTHERS VIA BLOGS, SOCIAL NETWORKS, OR JUST TALK ABOUT IT

Question HOW COMPANIES SAVE, STORE AND USE YOUR PERSONAL DATA

Learn ABOUT ONLINE PRIVACY AND KNOW YOUR RIGHTS!

Share WHAT YOU DISCOVER, EDUCATE OTHERS VIA BLOGS, SOCIAL NETWORKS, OR JUST TALK ABOUT IT

Explore RUN YOUR OWN SERVER, USE OPEN SOURCE TOOLS TO PROTECT YOURSELF WHILE HELPING OTHERS, IT'S FUN!

Contact PHILCRYER.COM

Slides BIT.LY/PC-SLIDES

Follow @FAK3R

Contact PHILCRYER.COM

Slides BIT.LY/PC-SLIDES

Follow @FAK3R

Thanks

EFF

ST LOUIS LINUX USERS GROUP

SBS CREATIX