BITS OF FREEDOM

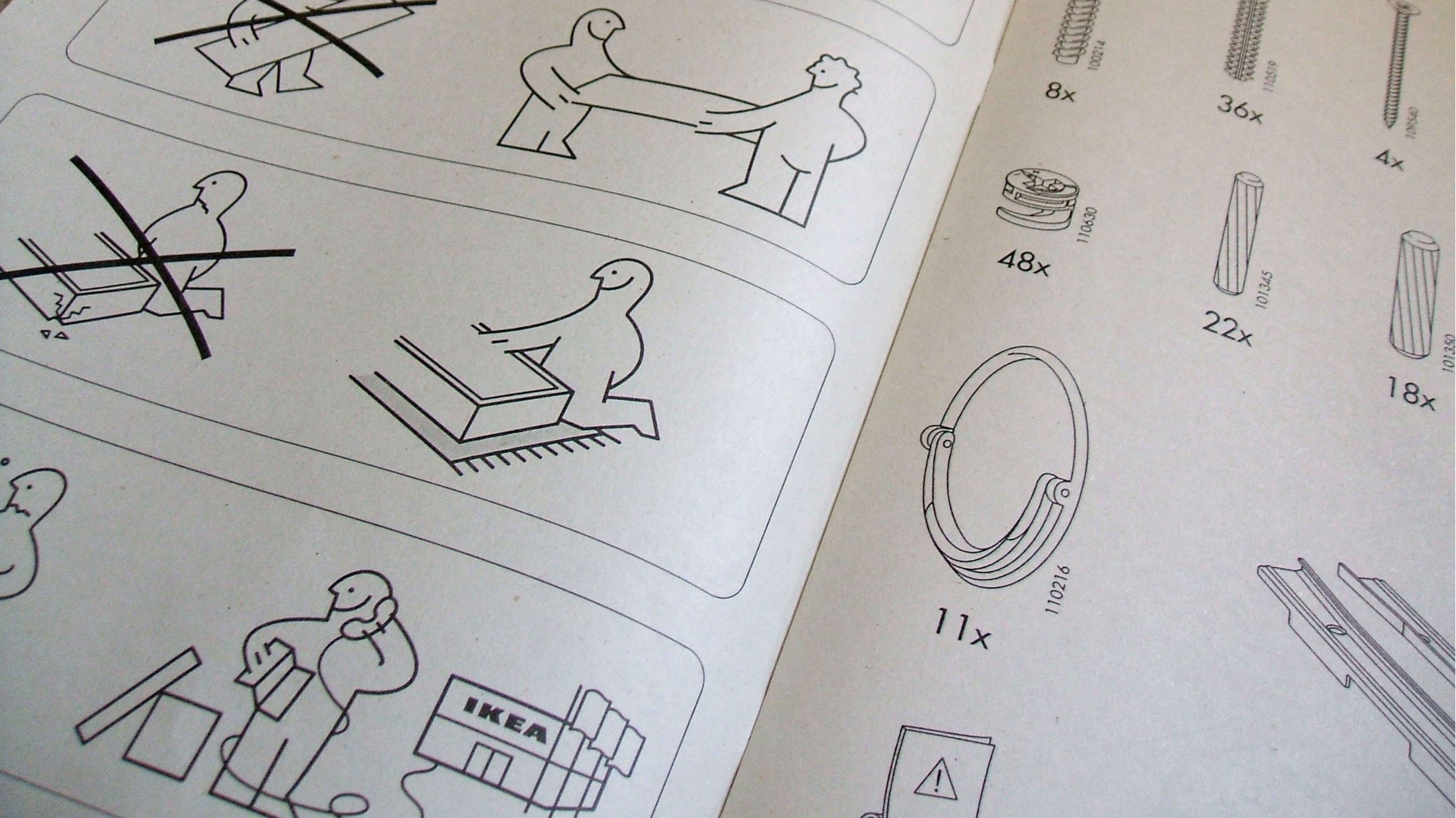
VERDEDIGT DIGITALE BURGERRECHTEN

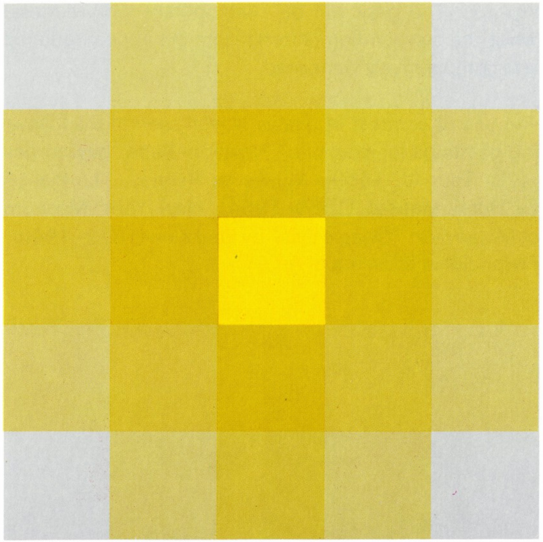
Rejo Zenger | rejo.zenger@bof.nl | @bitsoffreedom | @rejozenger

Big Brother Awards

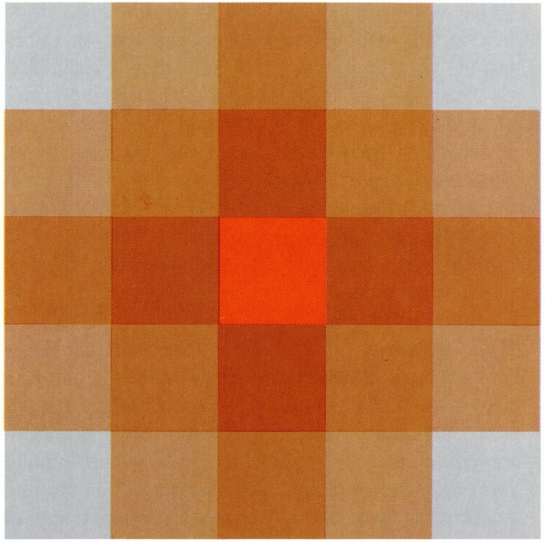
October 28th, 2015

Designing freedom

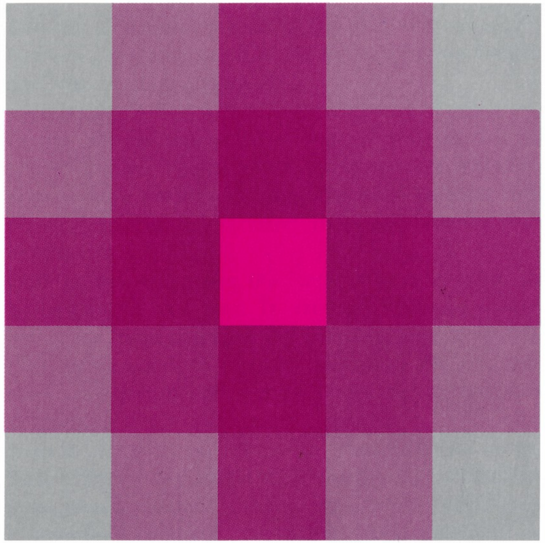

100214
8x
110519
36x
100540
4x
110630
48x
101345
22x
101350
18x
110216
11x
IKEA



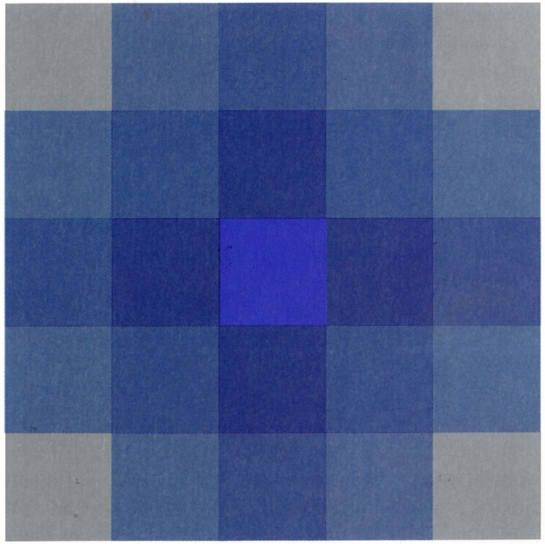
38



39



40



41

SAE

Marshall McLuhan

Technology is the extension of man

The medium is the message

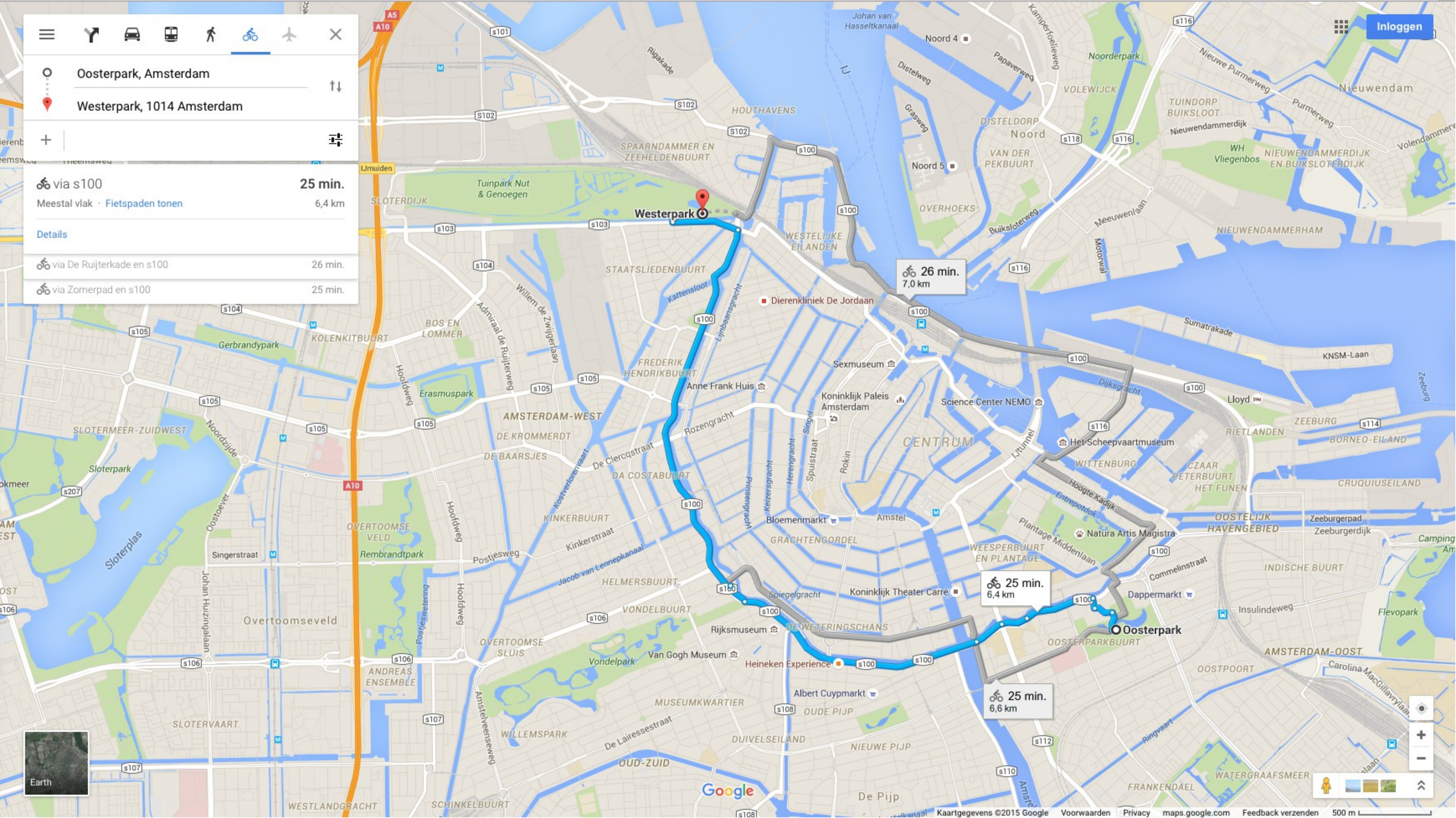
Figure and ground

Lawrence Lessig

Computer code regulates conduct in much the same way that legal code does.

Four major regulators: Laws, Norms, Market and Architecture.

Why relevant to freedom?



Oosterpark, Amsterdam

Westerpark, 1014 Amsterdam

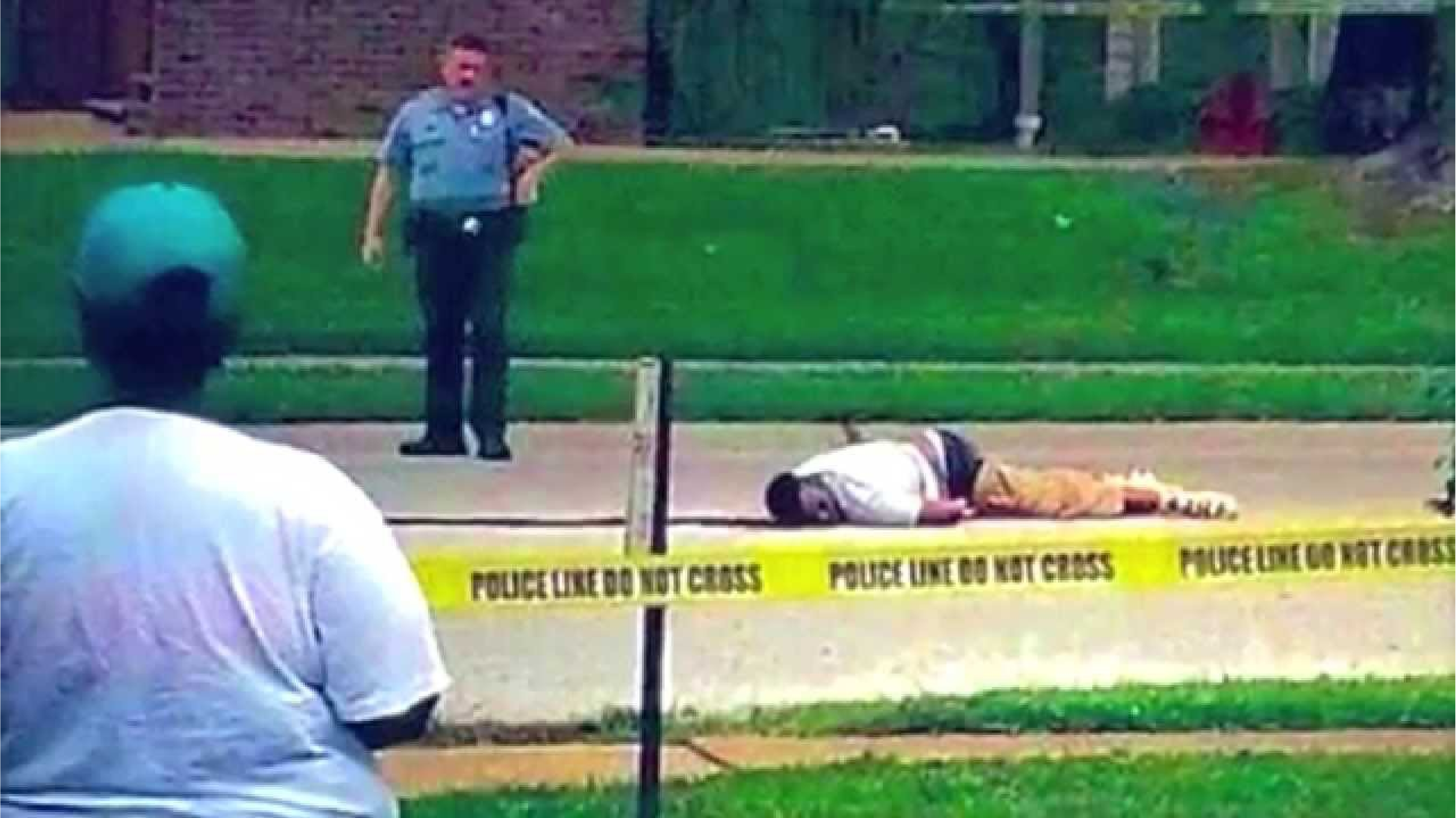
via s100 — 25 min.

Meestal vlak · Fietspaden tonen — 6,4 km

Details

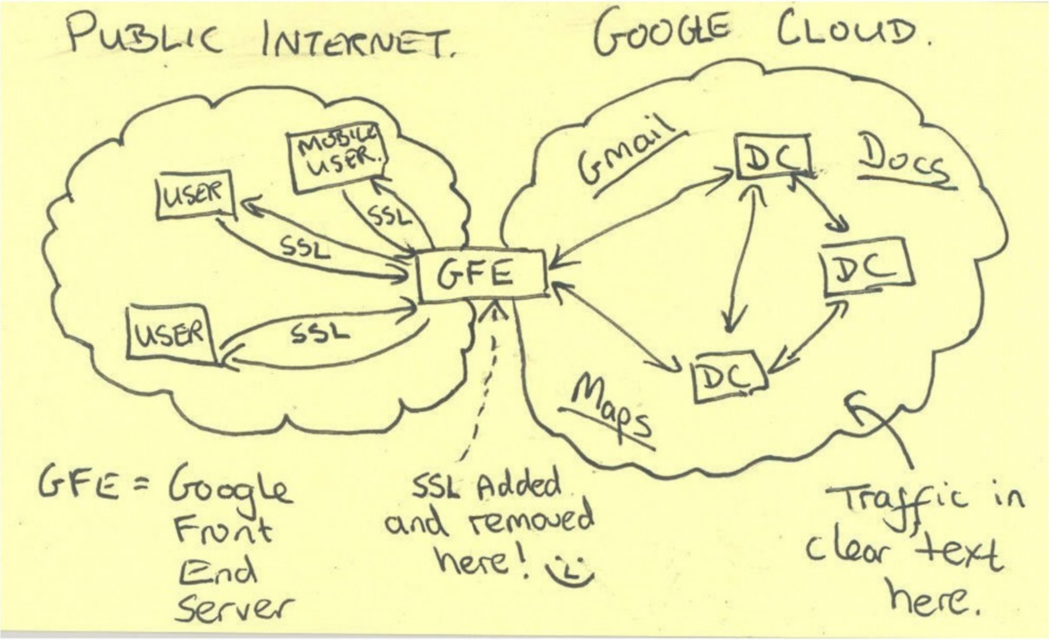
via De Ruijterkade en s100 — 26 min.

via Zomerpad en s100 — 25 min.


POLICE LINE DO NOT CROSS
POLICE LINE DO NOT CROSS
POLICE LINE DO NOT CROSS

HANDS UP DONT SHOOT
#JusticeForMikeBrown
HANDS UP DONT SHOOT
#JusticeForMikeBrown
HANDS UP DONT
#JusticeForMi

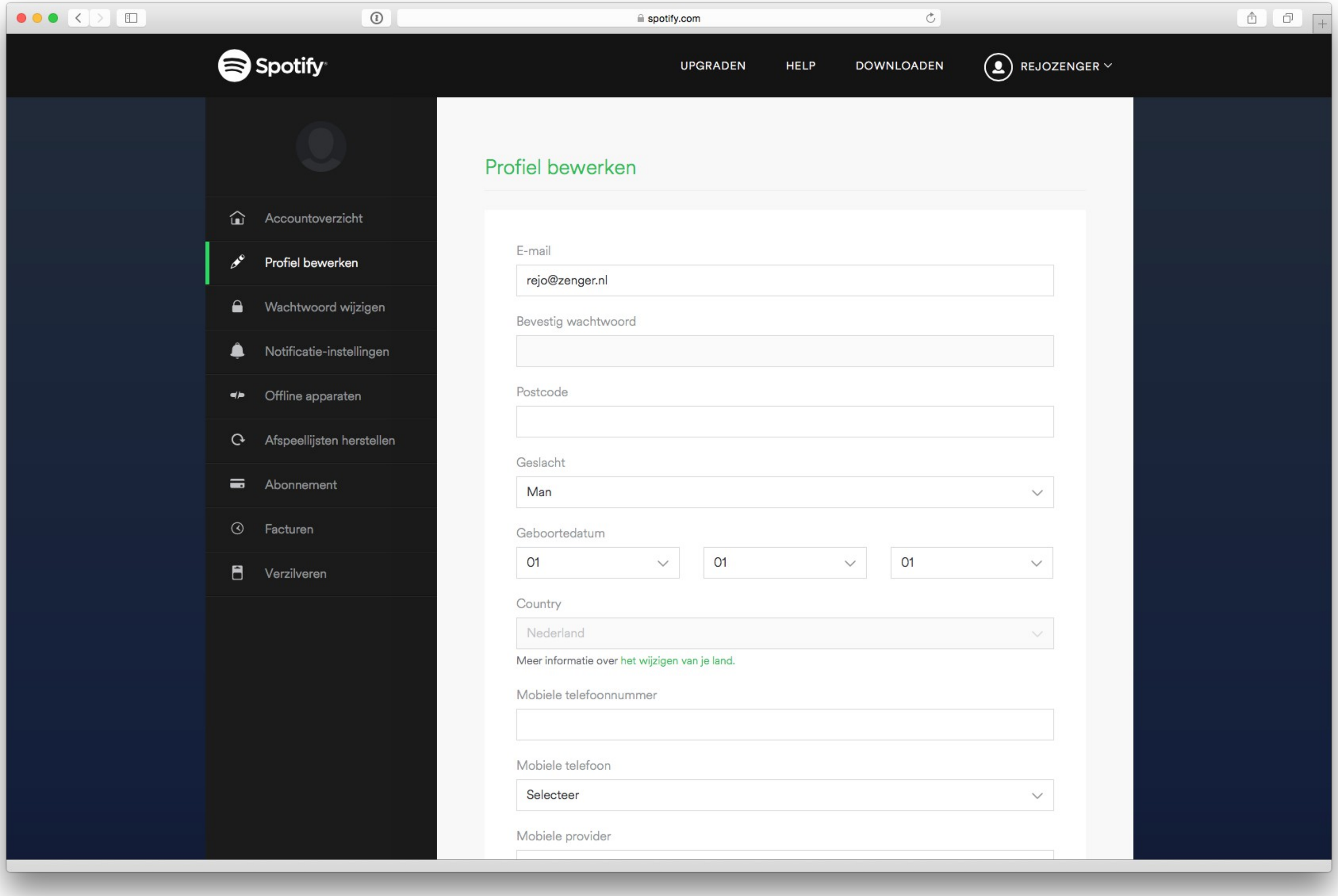
Current Efforts - Google


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

“There are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask though questions about what we should do.”

So, now what?

Don't ask for details you don't need.



Profiel bewerken

E-mail: rejo@zenger.nl

Bevestig wachtwoord:

Postcode:

Geslacht: Man

Geboortedatum: 01 01 01

Country: Nederland

Meer informatie over het wijzigen van je land.

Mobiele telefoonnummer:

Mobiele telefoon: Selecteer

Mobiele provider:

Decentralise whenever possible.

Zonnepanelen nu: 1390 Watt

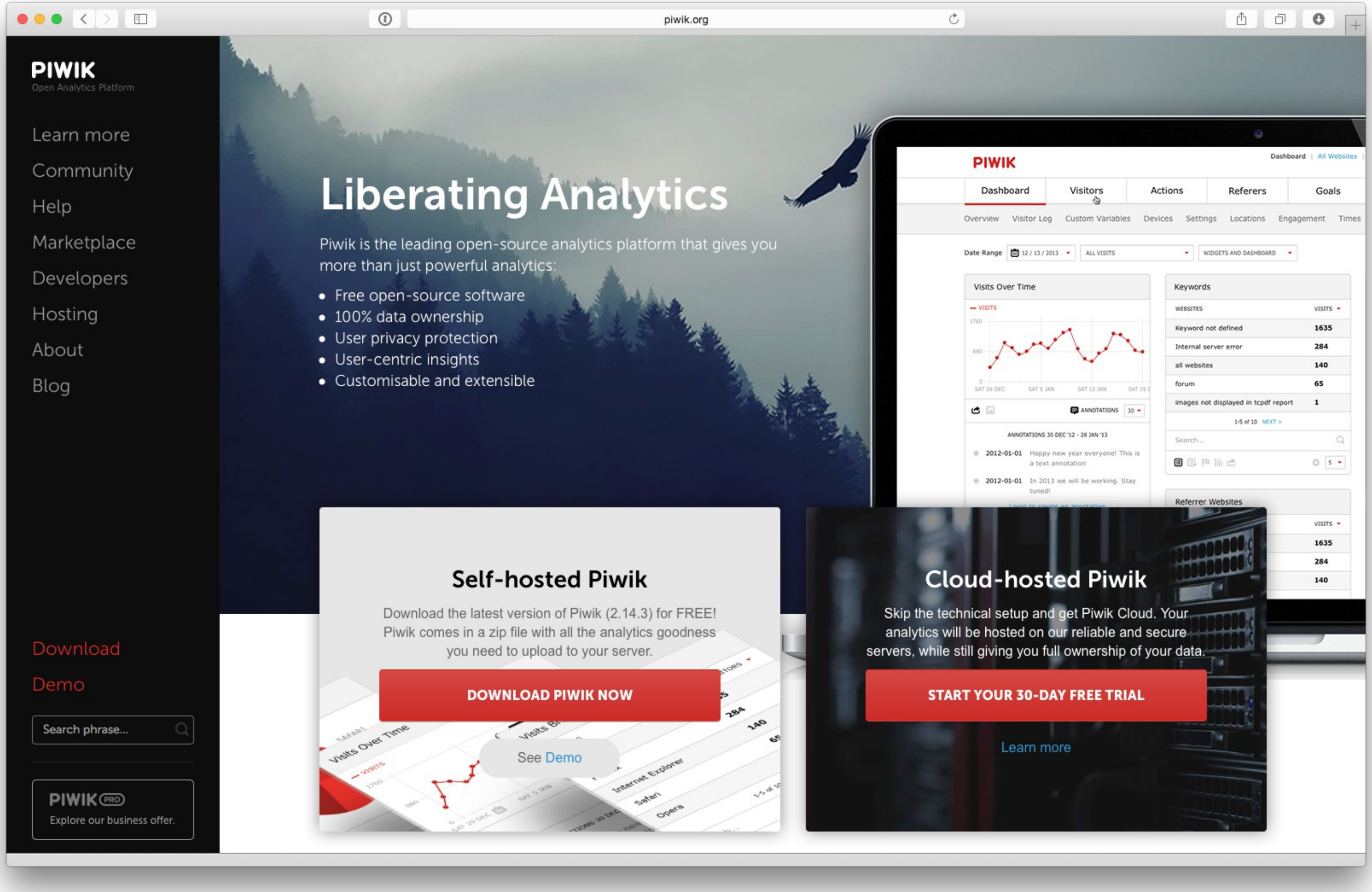
Verbruik nu: 843 Watt

Teruglevering nu: 547 Watt

18,0°

Volgt programma ▸ 19,0° om 20:00 uur op Comfort

Don't have others spy on your users.



PIWIK
Open Analytics Platform

- Learn more
- Community
- Help
- Marketplace
- Developers
- Hosting
- About
- Blog

Download

Demo

Search phrase...

PIWIK PRO
Explore our business offer.

Liberating Analytics

Piwik is the leading open-source analytics platform that gives you more than just powerful analytics:

- Free open-source software
- 100% data ownership
- User privacy protection
- User-centric insights
- Customisable and extensible

Self-hosted Piwik

Download the latest version of Piwik (2.14.3) for FREE! Piwik comes in a zip file with all the analytics goodness you need to upload to your server.

DOWNLOAD PIWIK NOW

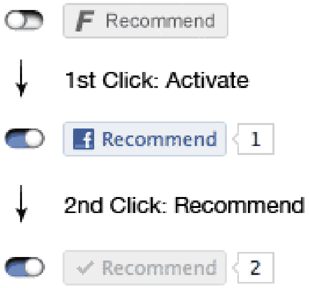
See Demo

Cloud-hosted Piwik

Skip the technical setup and get Piwik Cloud. Your analytics will be hosted on our reliable and secure servers, while still giving you full ownership of your data.

START YOUR 30-DAY FREE TRIAL

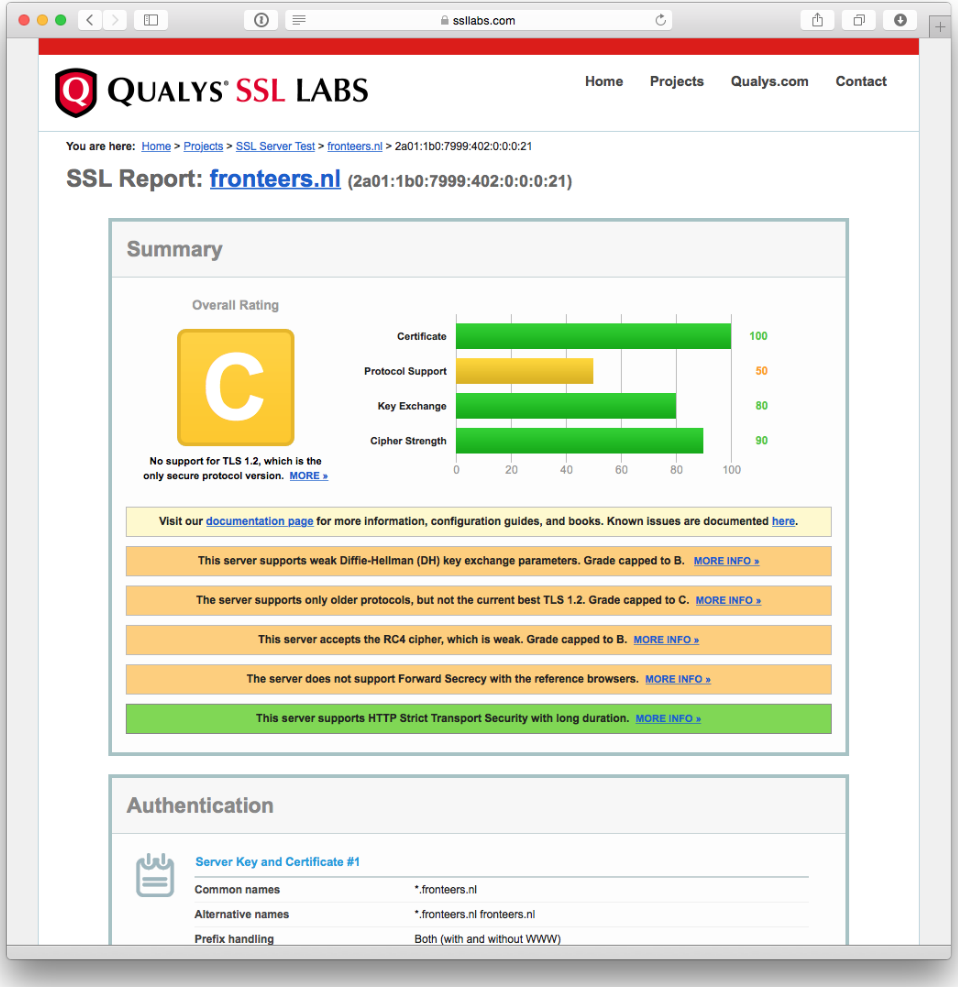
Learn more



1st Click: Activate

2nd Click: Recommend

Encrypt everything.



You are here: Home > Projects > SSL Server Test > fronteers.nl > 2a01:1b0:7999:402:0:0:0:21

SSL Report: fronteers.nl (2a01:1b0:7999:402:0:0:0:21)

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »

Certificate	100
Protocol Support	50
Key Exchange	80
Cipher Strength	90

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

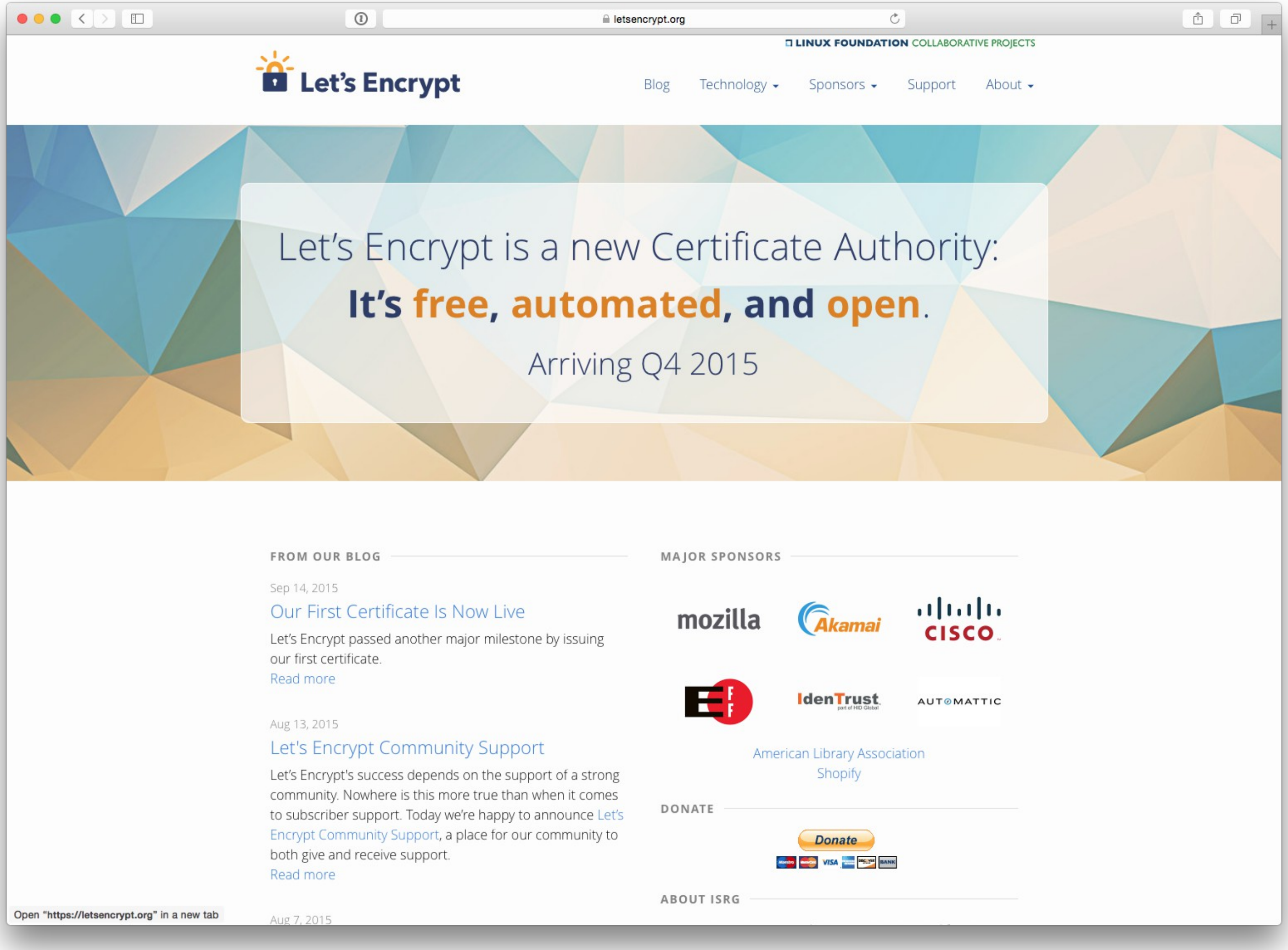
The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server supports HTTP Strict Transport Security with long duration. MORE INFO »

Authentication

Server Key and Certificate #1

Common names	*.fronteers.nl
Alternative names	*.fronteers.nl fronteers.nl
Prefix handling	Both (with and without WWW)



Let’s Encrypt is a new Certificate Authority:

It’s free, automated, and open.

Arriving Q4 2015

FROM OUR BLOG

Sep 14, 2015

Our First Certificate Is Now Live

Let’s Encrypt passed another major milestone by issuing our first certificate.

Read more

Aug 13, 2015

Let's Encrypt Community Support

Let’s Encrypt's success depends on the support of a strong community. Nowhere is this more true than when it comes to subscriber support. Today we’re happy to announce Let’s Encrypt Community Support, a place for our community to both give and receive support.

Read more

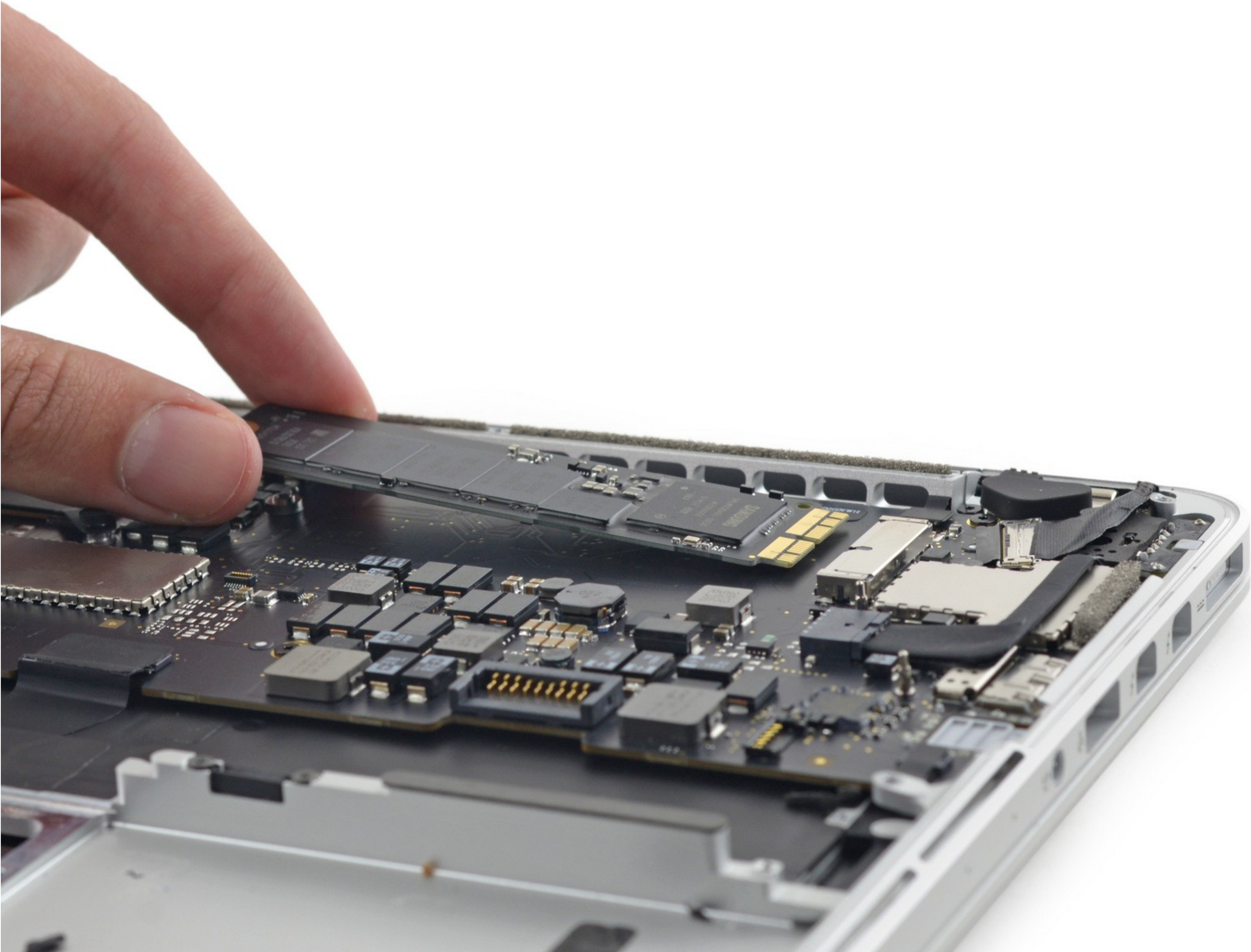
Aug 7, 2015

MAJOR SPONSORS

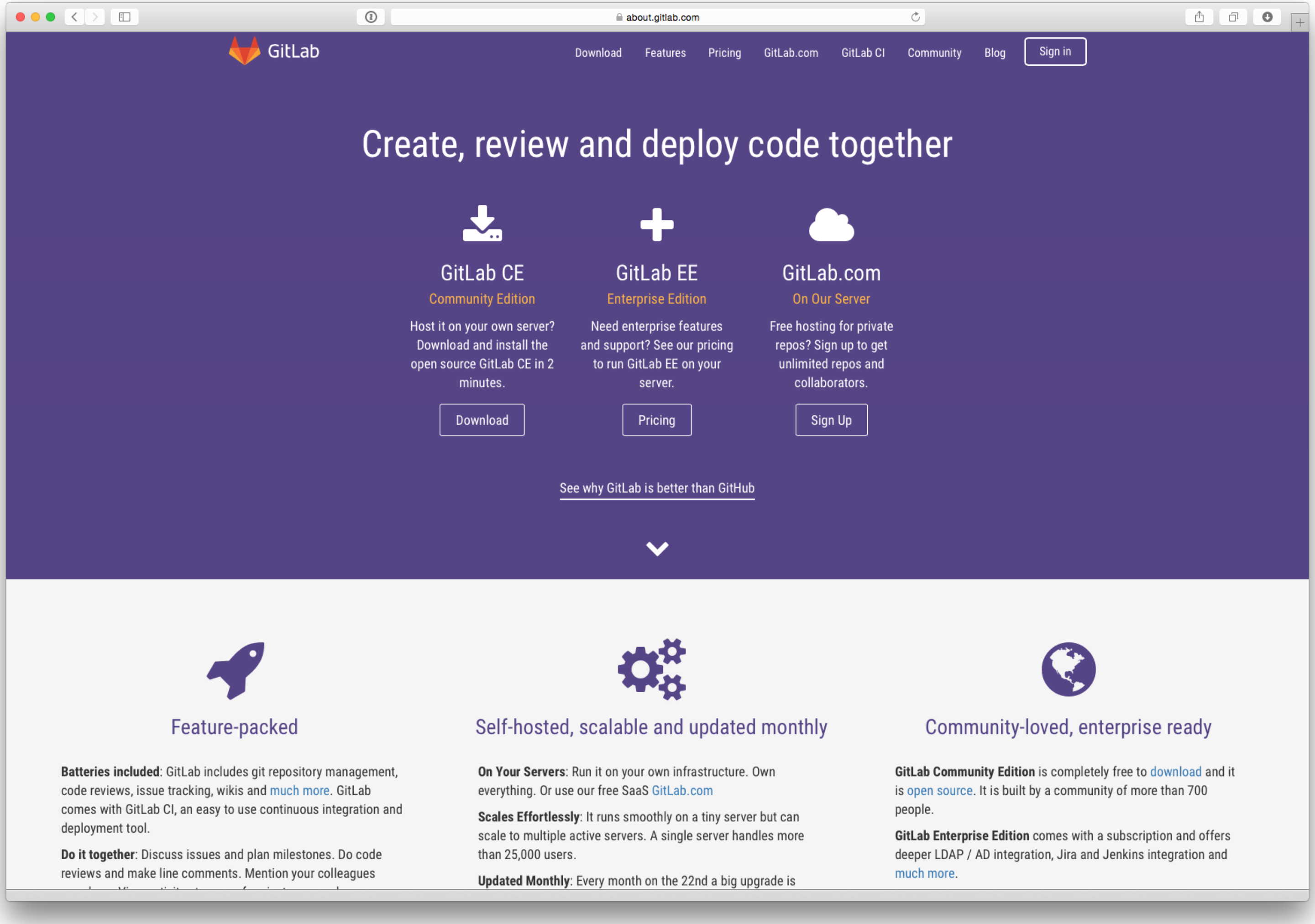
American Library Association
Shopify

DONATE

ABOUT ISRG


SAMSUNG

Host your own code.



Create, review and deploy code together

GitLab CE

Community Edition

Host it on your own server? Download and install the open source GitLab CE in 2 minutes.

GitLab EE

Enterprise Edition

Need enterprise features and support? See our pricing to run GitLab EE on your server.

GitLab.com

On Our Server

Free hosting for private repos? Sign up to get unlimited repos and collaborators.

See why GitLab is better than GitHub

Feature-packed

Batteries included: GitLab includes git repository management, code reviews, issue tracking, wikis and much more. GitLab comes with GitLab CI, an easy to use continuous integration and deployment tool.

Do it together: Discuss issues and plan milestones. Do code reviews and make line comments. Mention your colleagues

Self-hosted, scalable and updated monthly

On Your Servers: Run it on your own infrastructure. Own everything. Or use our free SaaS GitLab.com

Scales Effortlessly: It runs smoothly on a tiny server but can scale to multiple active servers. A single server handles more than 25,000 users.

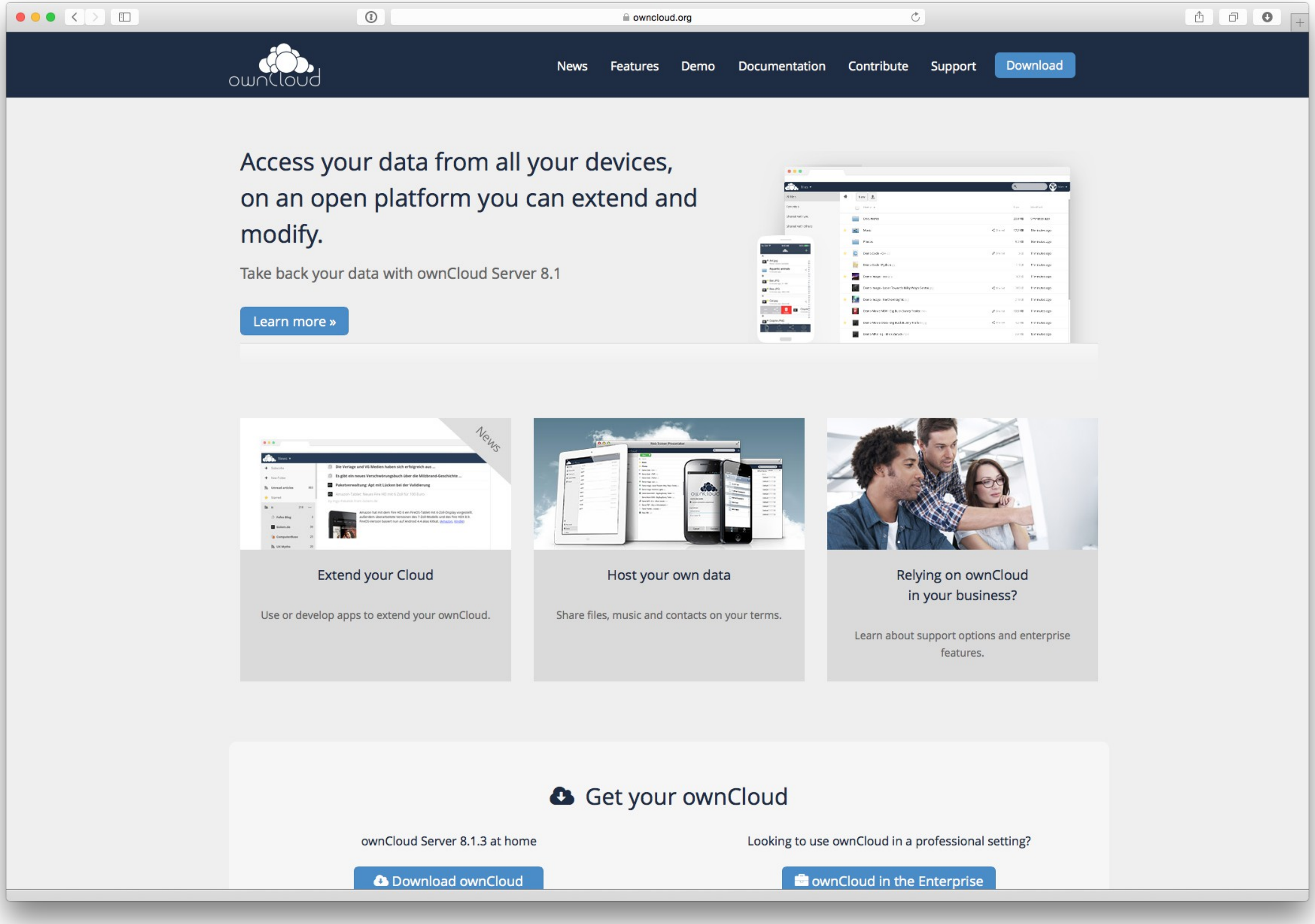
Updated Monthly: Every month on the 22nd a big upgrade is

Community-loved, enterprise ready

GitLab Community Edition is completely free to download and it is open source. It is built by a community of more than 700 people.

GitLab Enterprise Edition comes with a subscription and offers deeper LDAP / AD integration, Jira and Jenkins integration and much more.

Or even better:
own everything you do.



Access your data from all your devices, on an open platform you can extend and modify.

Take back your data with ownCloud Server 8.1

Extend your Cloud

Use or develop apps to extend your ownCloud.

Host your own data

Share files, music and contacts on your terms.

Relying on ownCloud in your business?

Learn about support options and enterprise features.

Get your ownCloud

ownCloud Server 8.1.3 at home

Looking to use ownCloud in a professional setting?

Be transparant to the user.

Author G [redacted] F [redacted] (10 [redacted]
Sent 2011-04-20 15:00:45 UTC
Body lieber [redacted]
Author M [redacted] S [redacted] (50 [redacted]
Sent 2011-04-20 19:01:54 UTC
Body [redacted]

Id 16 [redacted]
Subject
Folders [fb]messages, [fb]deleted, [fb]sent
Deleted true
Recipients M [redacted] S [redacted] (50 [redacted]
[redacted] [redacted] L [redacted] (50 [redacted]
Author [redacted] [redacted] L [redacted] (50 [redacted]
Sent 2011-04-13 22:28:32 UTC
Body hey [redacted]
Author M [redacted] S [redacted] (50 [redacted]
Sent 2011-04-13 22:30:08 UTC
Body huhu [redacted]
Author [redacted] [redacted] L [redacted] (50 [redacted]
Sent 2011-04-14 17:49:53 UTC
Body huhu [redacted]
Author [redacted] [redacted] L [redacted] (50 [redacted]
Sent 2011-04-18 21:16:53 UTC
Body hoff [redacted]
Author [redacted] [redacted] L [redacted] (50 [redacted]
Sent 2011-04-18 21:39:56 UTC
Body damit [redacted]

Story M [redacted] S [redacted] likes I [redacted] A [redacted] R [redacted]

Name

First M [redacted]
Middle
Last S [redacted]

Name Changes

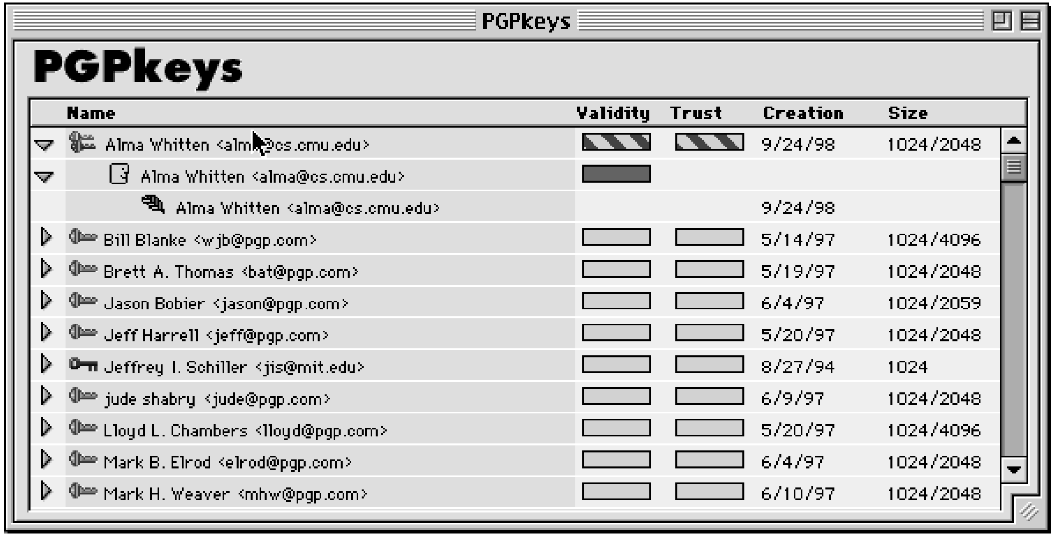
Time 2010-03-19 11:48:50 UTC
Old Name M [redacted] S [redacted]
New Name M [redacted] c [redacted]
Time 2010-06-17 22:10:35 UTC
Old Name M [redacted] c [redacted]
New Name M [redacted] ш [redacted]
Time 2010-10-29 08:59:36 UTC
Old Name M [redacted] ш [redacted]
New Name M [redacted] S [redacted]

Networks

Notes

Title [redacted] Ü [redacted]
Link [redacted]
Created 2010-09-01 08:44:02 UTC
Updated 2010-09-01 08:44:02 UTC
Tags
Text A [redacted]

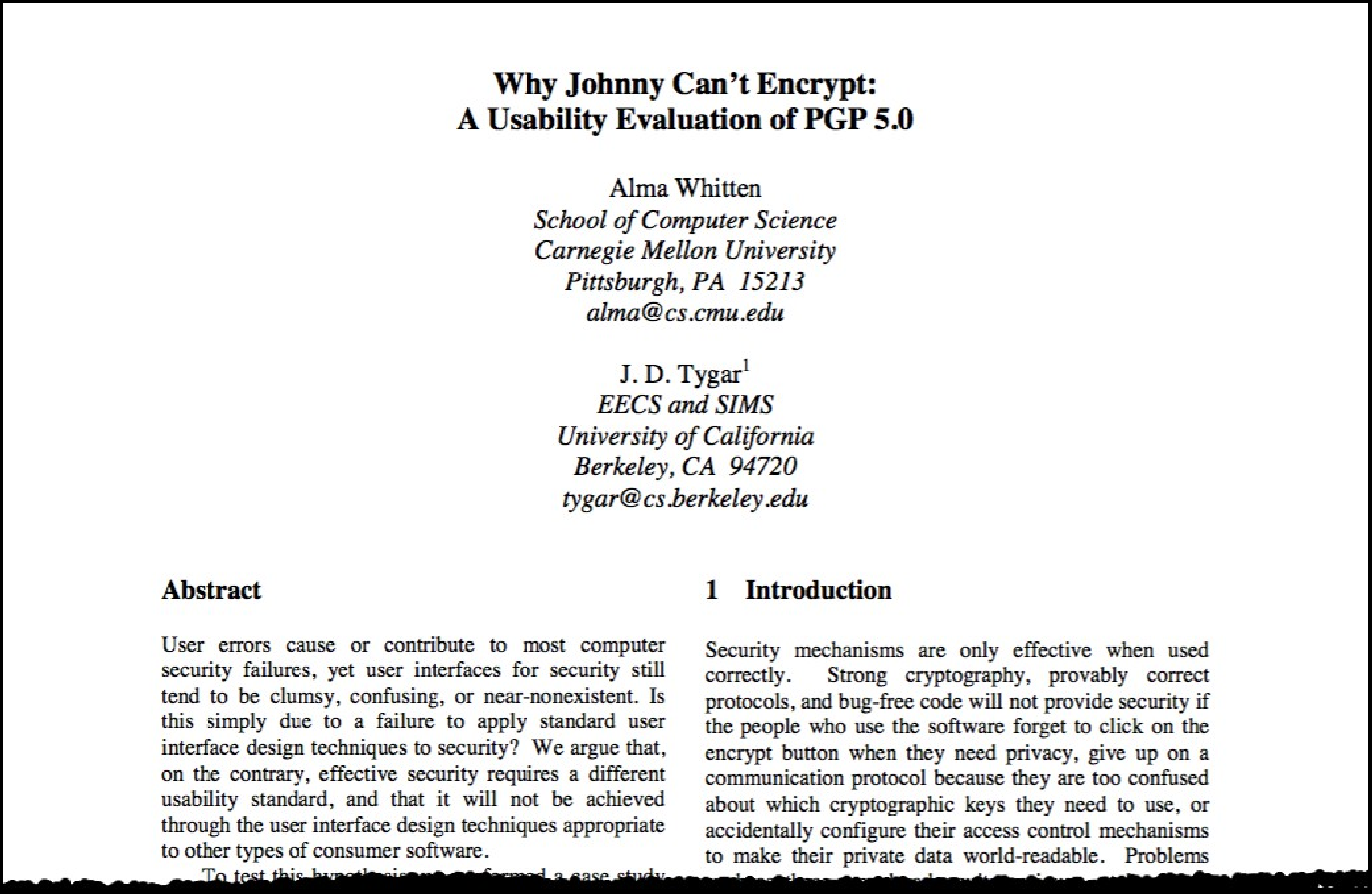
It's useable when
your user thinks it is.



PGPkeys

PGPkeys

Name	Validity	Trust	Creation	Size
Alma Whitten <alma@cs.cmu.edu>	▨	▨	9/24/98	1024/2048
Alma Whitten <alma@cs.cmu.edu>	■			
Alma Whitten <alma@cs.cmu.edu>			9/24/98	
Bill Blanke <wjb@pgp.com>	□	□	5/14/97	1024/4096
Brett A. Thomas <bat@pgp.com>	□	□	5/19/97	1024/2048
Jason Bobier <jason@pgp.com>	□	□	6/4/97	1024/2059
Jeff Harrell <jeff@pgp.com>	□	□	5/20/97	1024/2048
Jeffrey I. Schiller <jis@mit.edu>	□	□	8/27/94	1024
jude shabry <jude@pgp.com>	□	□	6/9/97	1024/2048
Lloyd L. Chambers <lloyd@pgp.com>	□	□	5/20/97	1024/4096
Mark B. Elrod <elrod@pgp.com>	□	□	6/4/97	1024/2048
Mark H. Weaver <mhw@pgp.com>	□	□	6/10/97	1024/2048



Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

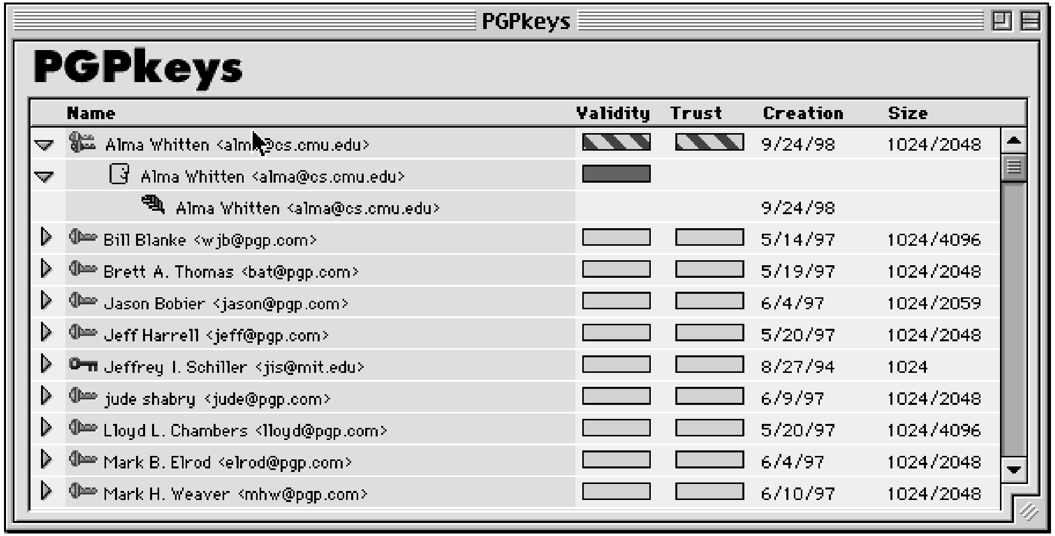
Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis we performed a case study

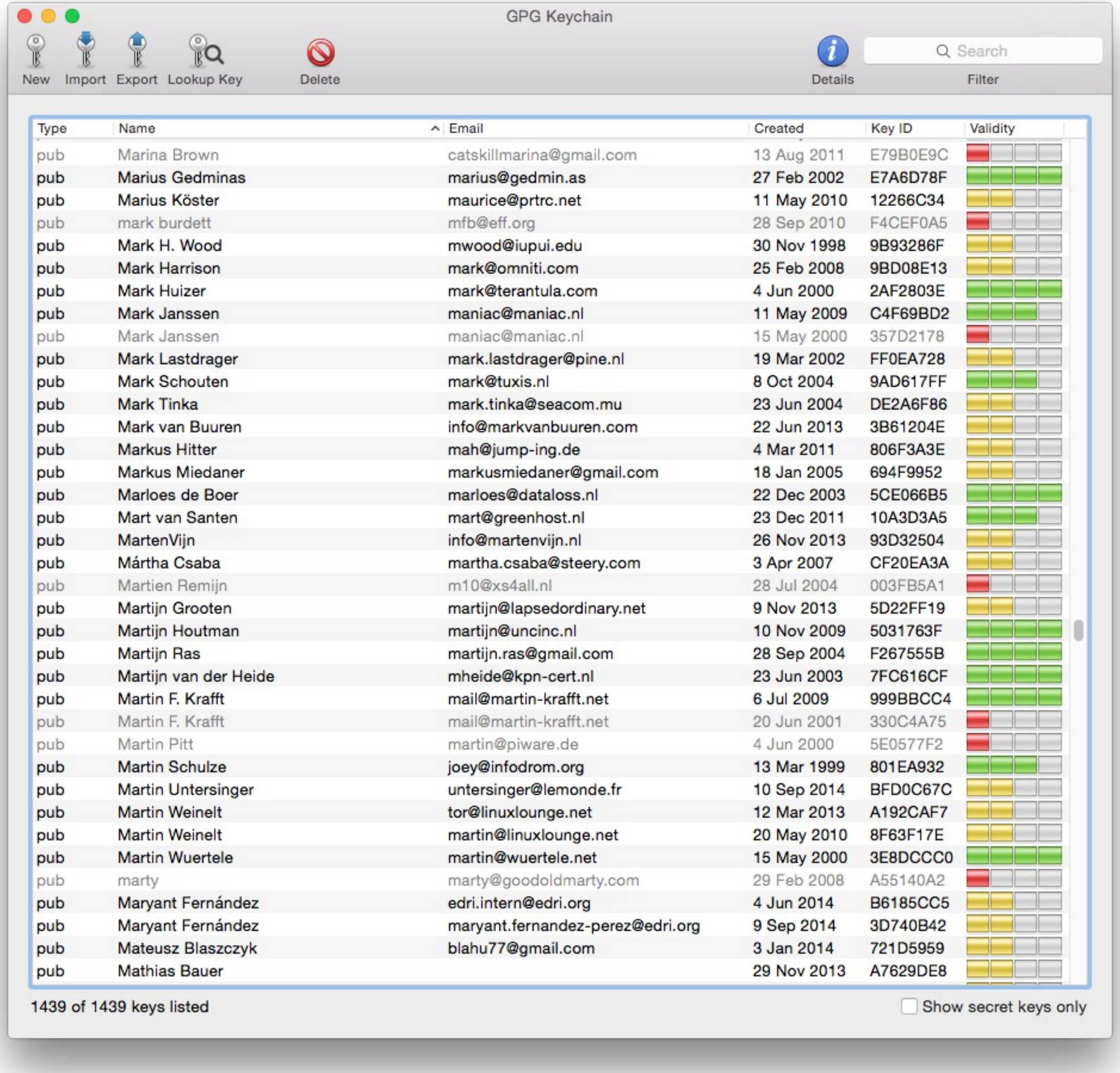
1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems



PGPkeys

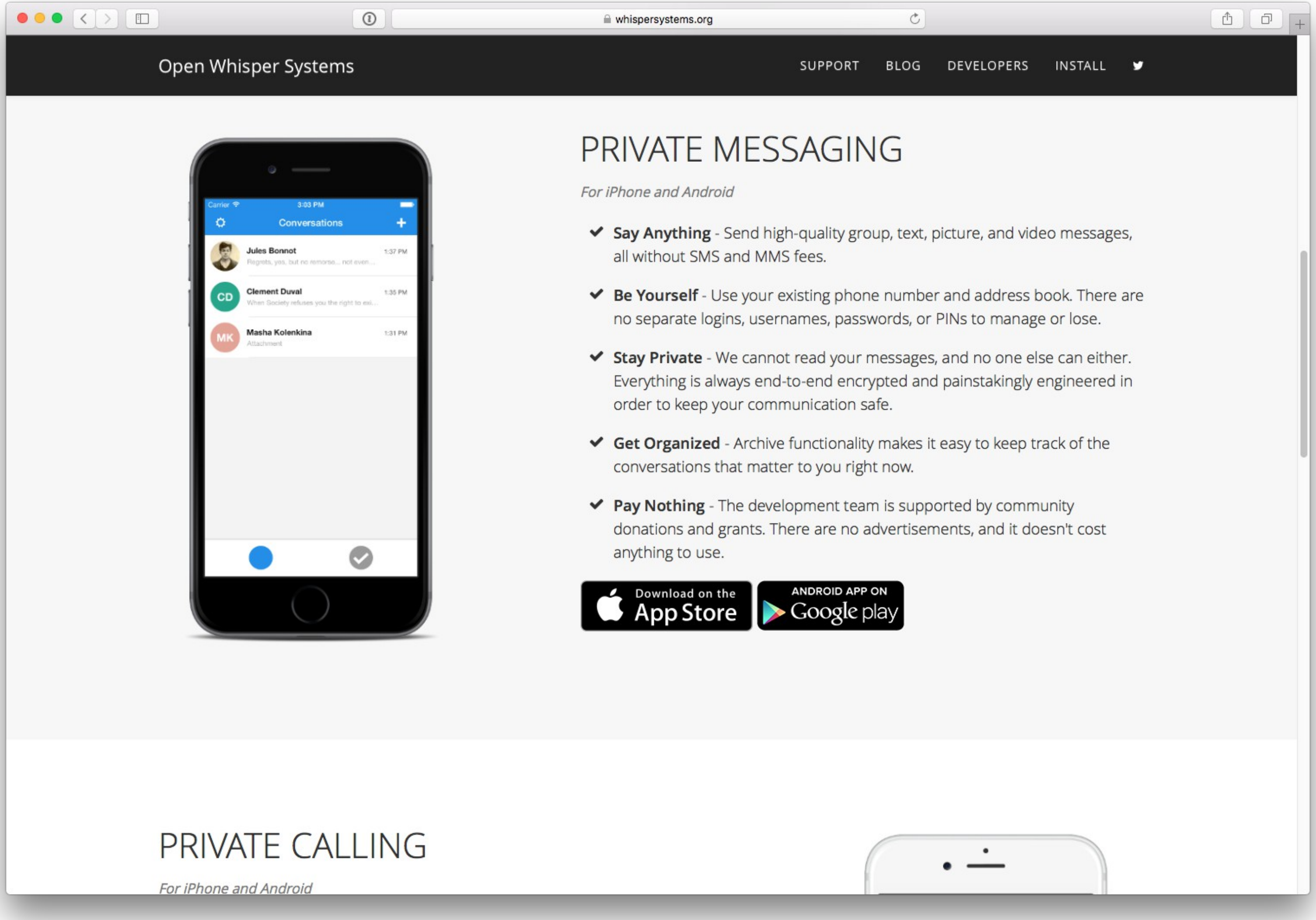
Name	Validity	Trust	Creation	Size
Alma Whitten <alma@cs.cmu.edu>	▨	▨	9/24/98	1024/2048
Alma Whitten <alma@cs.cmu.edu>	■			
Alma Whitten <alma@cs.cmu.edu>			9/24/98	
Bill Blanke <wjb@pgp.com>	□	□	5/14/97	1024/4096
Brett A. Thomas <bat@pgp.com>	□	□	5/19/97	1024/2048
Jason Bobier <jason@pgp.com>	□	□	6/4/97	1024/2059
Jeff Harrell <jeff@pgp.com>	□	□	5/20/97	1024/2048
Jeffrey I. Schiller <jis@mit.edu>	□	□	8/27/94	1024
jude shabry <jude@pgp.com>	□	□	6/9/97	1024/2048
Lloyd L. Chambers <lloyd@pgp.com>	□	□	5/20/97	1024/4096
Mark B. Elrod <elrod@pgp.com>	□	□	6/4/97	1024/2048
Mark H. Weaver <mhw@pgp.com>	□	□	6/10/97	1024/2048



Type	Name	Email	Created	Key ID	Validity
pub	Marina Brown	catskillmarina@gmail.com	13 Aug 2011	E79B0E9C	🟥⬜⬜⬜
pub	Marius Gedminas	marius@gedmin.as	27 Feb 2002	E7A6D78F	🟩🟩🟩🟩
pub	Marius Köster	maurice@prtrc.net	11 May 2010	12266C34	🟨🟨⬜⬜
pub	mark burdett	mfb@eff.org	28 Sep 2010	F4CEF0A5	🟥⬜⬜⬜
pub	Mark H. Wood	mwood@iupui.edu	30 Nov 1998	9B93286F	🟨🟨⬜⬜
pub	Mark Harrison	mark@omniti.com	25 Feb 2008	9BD08E13	🟨🟨⬜⬜
pub	Mark Huizer	mark@terantula.com	4 Jun 2000	2AF2803E	🟩🟩🟩🟩
pub	Mark Janssen	maniac@maniac.nl	11 May 2009	C4F69BD2	🟩🟩🟩⬜
pub	Mark Janssen	maniac@maniac.nl	15 May 2000	357D2178	🟥⬜⬜⬜
pub	Mark Lastdrager	mark.lastdrager@pine.nl	19 Mar 2002	FF0EA728	🟨🟨⬜⬜
pub	Mark Schouten	mark@tuxis.nl	8 Oct 2004	9AD617FF	🟩🟩🟩⬜
pub	Mark Tinka	mark.tinka@seacom.mu	23 Jun 2004	DE2A6F86	🟨🟨⬜⬜
pub	Mark van Buuren	info@markvanbuuren.com	22 Jun 2013	3B61204E	🟨🟨⬜⬜
pub	Markus Hitter	mah@jump-ing.de	4 Mar 2011	806F3A3E	🟨🟨⬜⬜
pub	Markus Miedaner	markusmiedaner@gmail.com	18 Jan 2005	694F9952	🟨🟨⬜⬜
pub	Marloes de Boer	marloes@dataloss.nl	22 Dec 2003	5CE066B5	🟩🟩🟩🟩
pub	Mart van Santen	mart@greenhost.nl	23 Dec 2011	10A3D3A5	🟩🟩🟩⬜
pub	MartenVijn	info@martenvijn.nl	26 Nov 2013	93D32504	🟨🟨⬜⬜
pub	Mártha Csaba	martha.csaba@steery.com	3 Apr 2007	CF20EA3A	🟨🟨⬜⬜
pub	Martien Remijn	m10@xs4all.nl	28 Jul 2004	003FB5A1	🟥⬜⬜⬜
pub	Martijn Grooten	martijn@lapsedordinary.net	9 Nov 2013	5D22FF19	🟨🟨⬜⬜
pub	Martijn Houtman	martijn@uncinc.nl	10 Nov 2009	5031763F	🟩🟩🟩🟩
pub	Martijn Ras	martijn.ras@gmail.com	28 Sep 2004	F267555B	🟩🟩🟩🟩
pub	Martijn van der Heide	mheide@kpn-cert.nl	23 Jun 2003	7FC616CF	🟩🟩🟩🟩
pub	Martin F. Krafft	mail@martin-krafft.net	6 Jul 2009	999BBCC4	🟩🟩🟩🟩
pub	Martin F. Krafft	mail@martin-krafft.net	20 Jun 2001	330C4A75	🟥⬜⬜⬜
pub	Martin Pitt	martin@piware.de	4 Jun 2000	5E0577F2	🟥⬜⬜⬜
pub	Martin Schulze	joey@infodrom.org	13 Mar 1999	801EA932	🟩🟩🟩⬜
pub	Martin Untersinger	untersinger@lemonde.fr	10 Sep 2014	BFD0C67C	🟨🟨⬜⬜
pub	Martin Weinelt	tor@linuxlounge.net	12 Mar 2013	A192CAF7	🟨🟨⬜⬜
pub	Martin Weinelt	martin@linuxlounge.net	20 May 2010	8F63F17E	🟨🟨⬜⬜
pub	Martin Wuertele	martin@wuertele.net	15 May 2000	3E8DCCC0	🟩🟩🟩🟩
pub	marty	marty@goodoldmarty.com	29 Feb 2008	A55140A2	🟥⬜⬜⬜
pub	Maryant Fernández	edri.intern@edri.org	4 Jun 2014	B6185CC5	🟨🟨⬜⬜
pub	Maryant Fernández	maryant.fernandez-perez@edri.org	9 Sep 2014	3D740B42	🟨🟨⬜⬜
pub	Mateusz Blaszczyk	blahu77@gmail.com	3 Jan 2014	721D5959	🟨🟨⬜⬜
pub	Mathias Bauer		29 Nov 2013	A7629DE8	🟨🟨⬜⬜

1439 of 1439 keys listed

☐ Show secret keys only



Open Whisper Systems

SUPPORT BLOG DEVELOPERS INSTALL

PRIVATE MESSAGING

For iPhone and Android

✓ **Say Anything** - Send high-quality group, text, picture, and video messages, all without SMS and MMS fees.

✓ **Be Yourself** - Use your existing phone number and address book. There are no separate logins, usernames, passwords, or PINs to manage or lose.

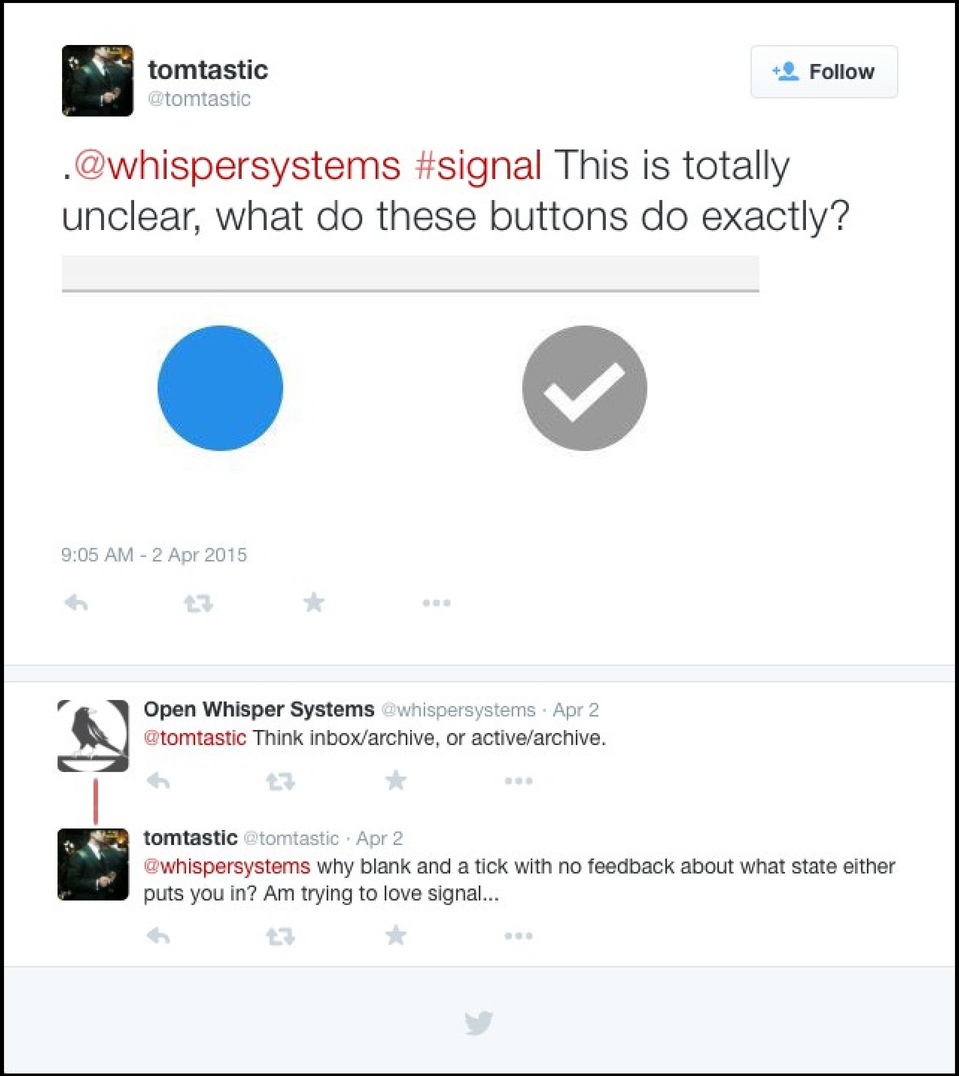
✓ **Stay Private** - We cannot read your messages, and no one else can either. Everything is always end-to-end encrypted and painstakingly engineered in order to keep your communication safe.

✓ **Get Organized** - Archive functionality makes it easy to keep track of the conversations that matter to you right now.

✓ **Pay Nothing** - The development team is supported by community donations and grants. There are no advertisements, and it doesn't cost anything to use.

PRIVATE CALLING

For iPhone and Android



tomtastic
@tomtastic

.@whispersystems #signal This is totally unclear, what do these buttons do exactly?

9:05 AM - 2 Apr 2015

Open Whisper Systems @whispersystems · Apr 2
@tomtastic Think inbox/archive, or active/archive.

tomtastic @tomtastic · Apr 2
@whispersystems why blank and a tick with no feedback about what state either puts you in? Am trying to love signal...

Or help your local digital rights organisation. There are many.

access

OPEN
RIGHTS
GROUP

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

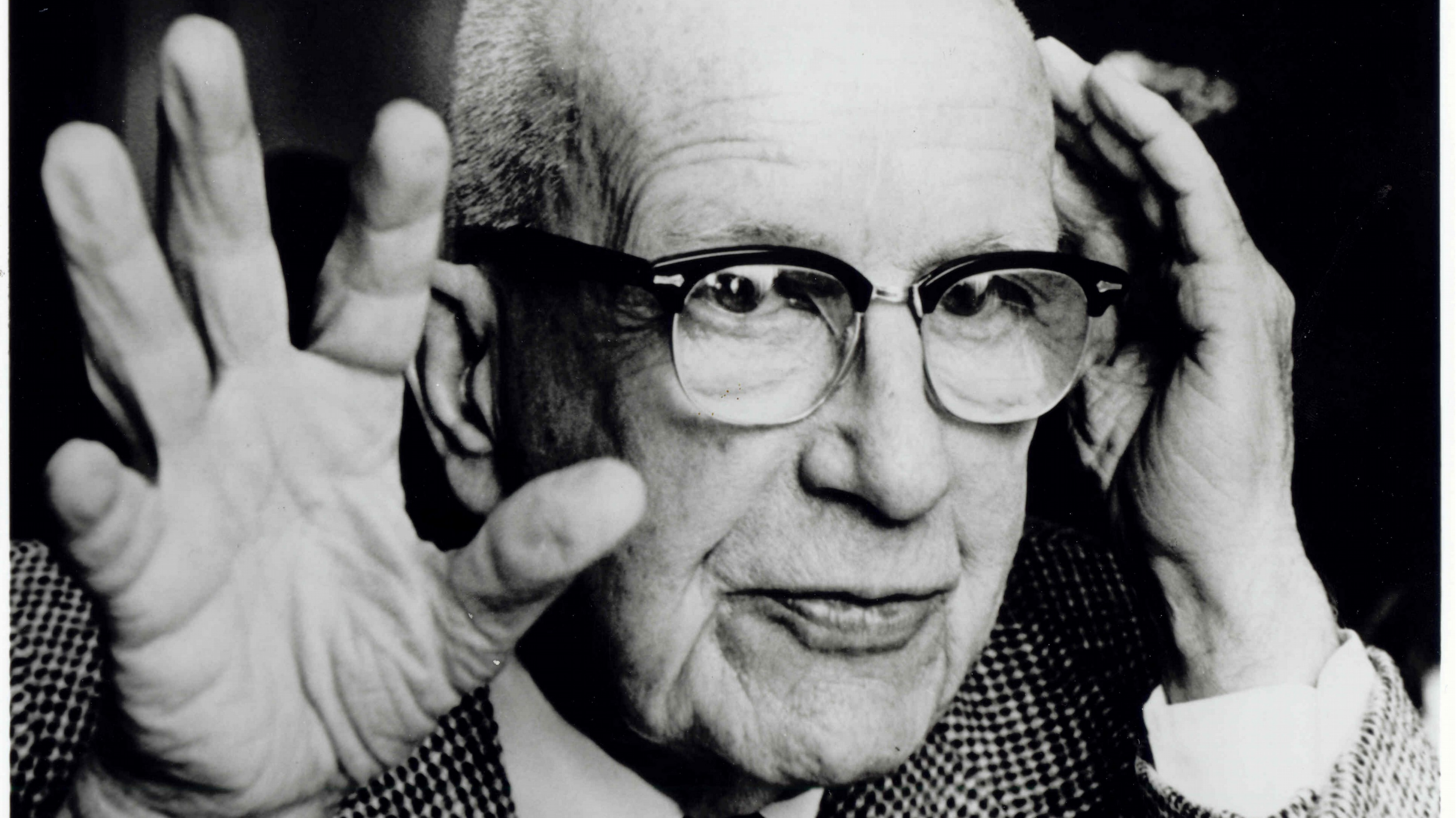
EDRi

PROTECTING DIGITAL FREEDOM

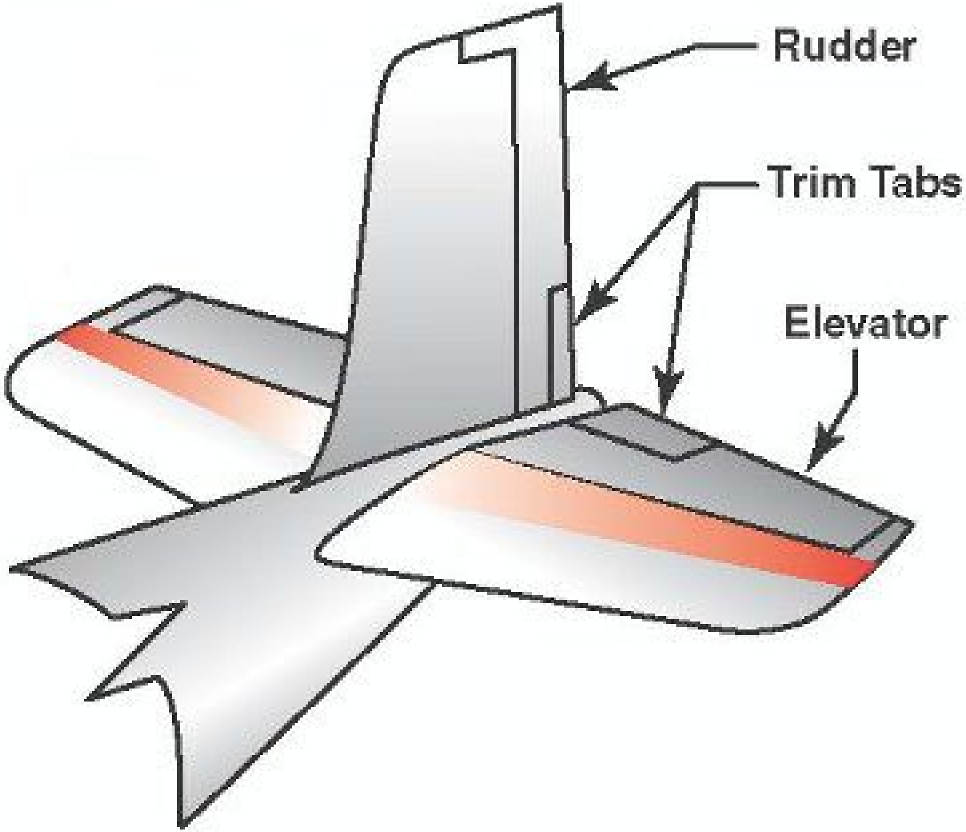
~~PRIVACY~~
~~INTERNATIONAL~~

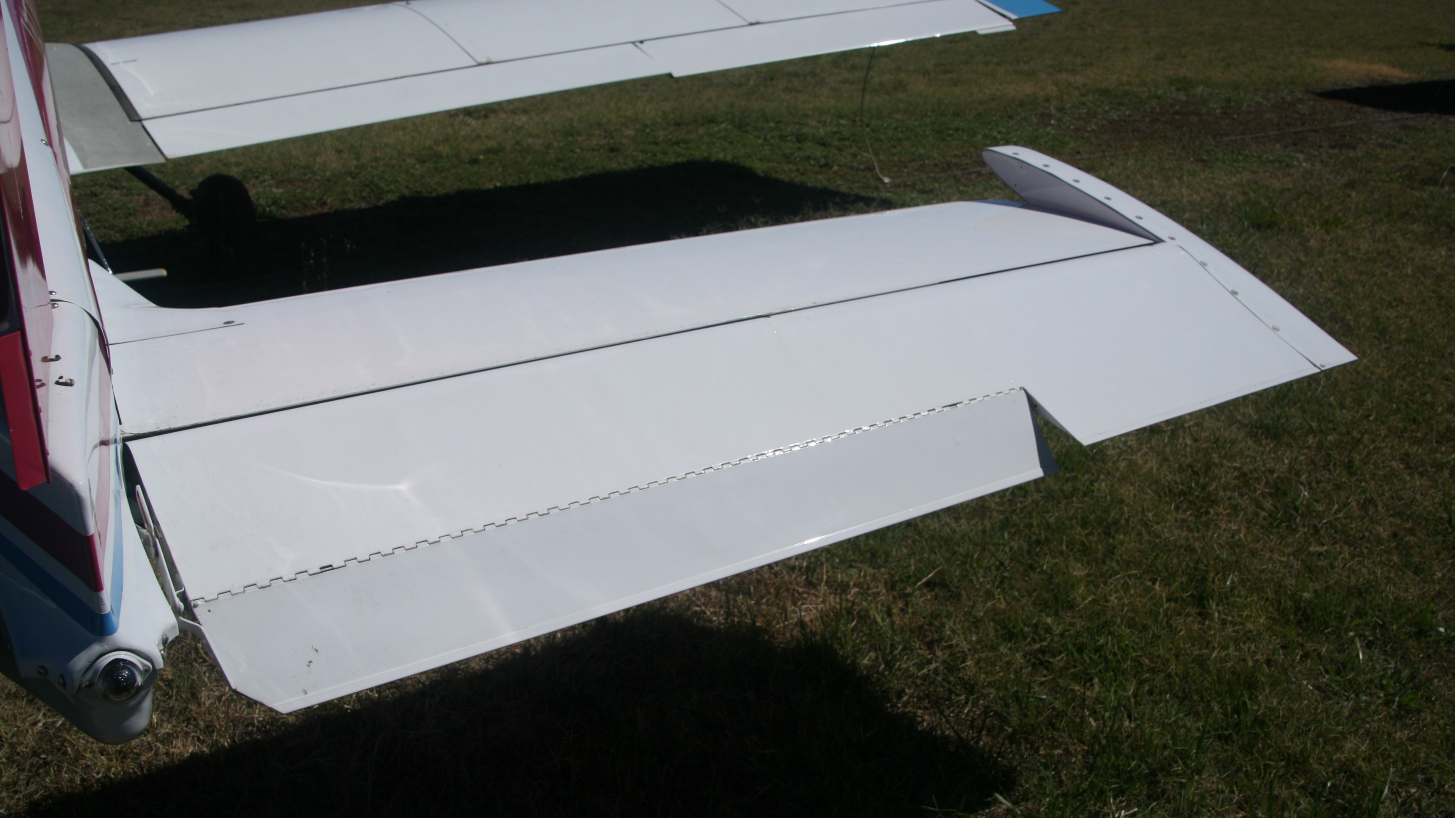
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

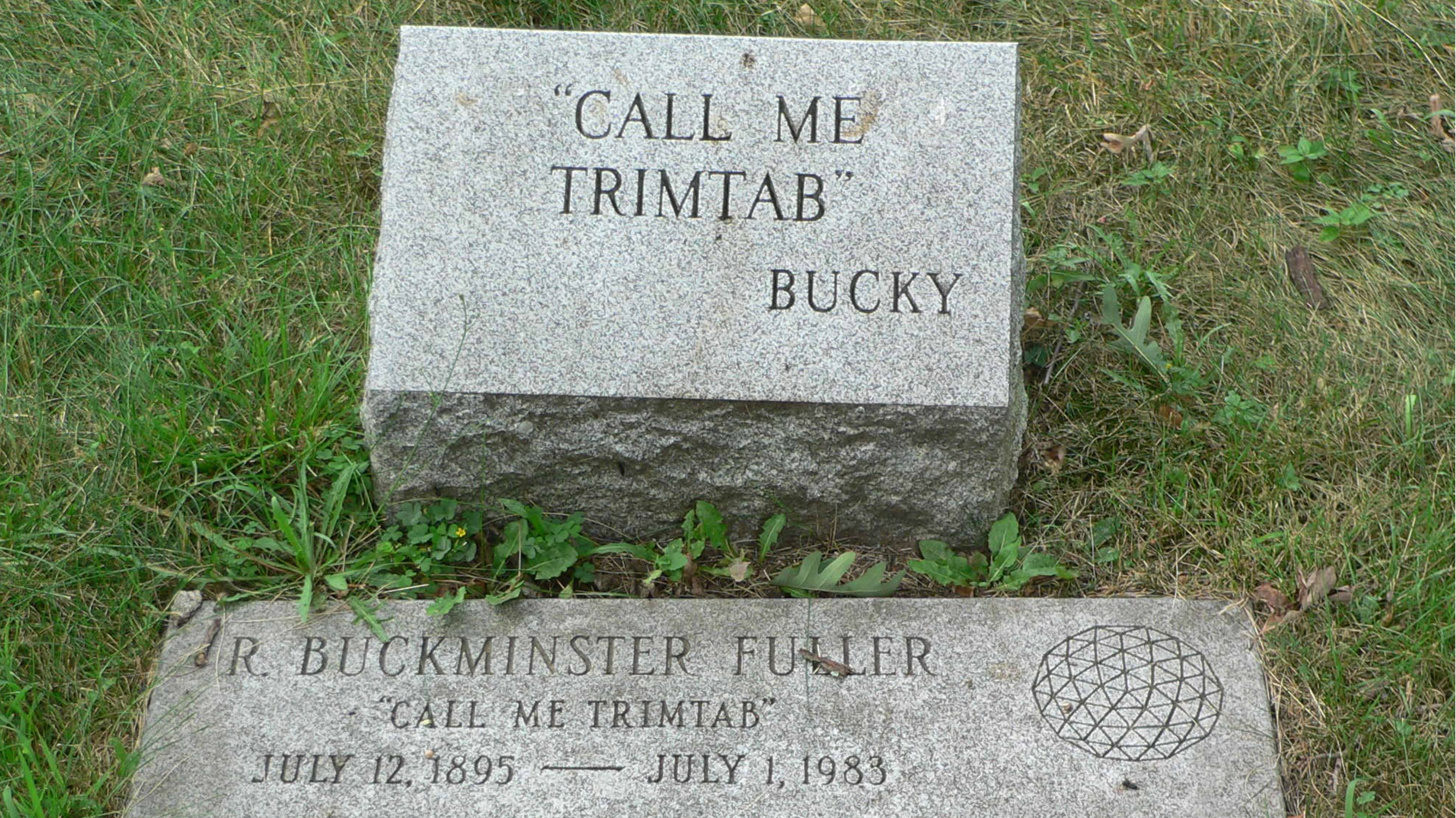
Who? Me?



YORK
NEW-YORK
NEW YORK
NEW YORK


Rudder
Trim Tabs
Elevator




"CALL ME
TRIMTAB"
BUCKY
R. BUCKMINSTER FULLER
"CALL ME TRIMTAB"
JULY 12, 1895 —— JULY 1, 1983

Now: question everything.

BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

Rejo Zenger | rejo.zenger@bof.nl | @bitsoffreedom | @rejozenger

Credits. Sze Ning (waterpump), Sze Ning (bad waterpump), J.T. Broekhuijse (good waterpump), Leif K-Brooks (Marshall McLuhan), Samwoo E (knife), Niklas Pivic (finger), Joi Ito (Lawrence Lessig), City Clock Magazine (Paris), Dylan Passmore (speed hump), Thomas Mulders (bagage claim), Kenny Louie (Ontario Highway 401), Getty (Ferguson protest), Lassi Kurkijärvi (Amsterdam), Edward Snowden (Platon for Wired), Barack Obama (himself), Fred Blocher (Buckminster Fuller), YSSYguy (trimtab of Plane) and Shriramk (Bucky's grave).