Open Source Software As Activism

March 4, 2017

Dr. Christine Corbett Moran
corbett@caltech.edu

California Institute of Technology

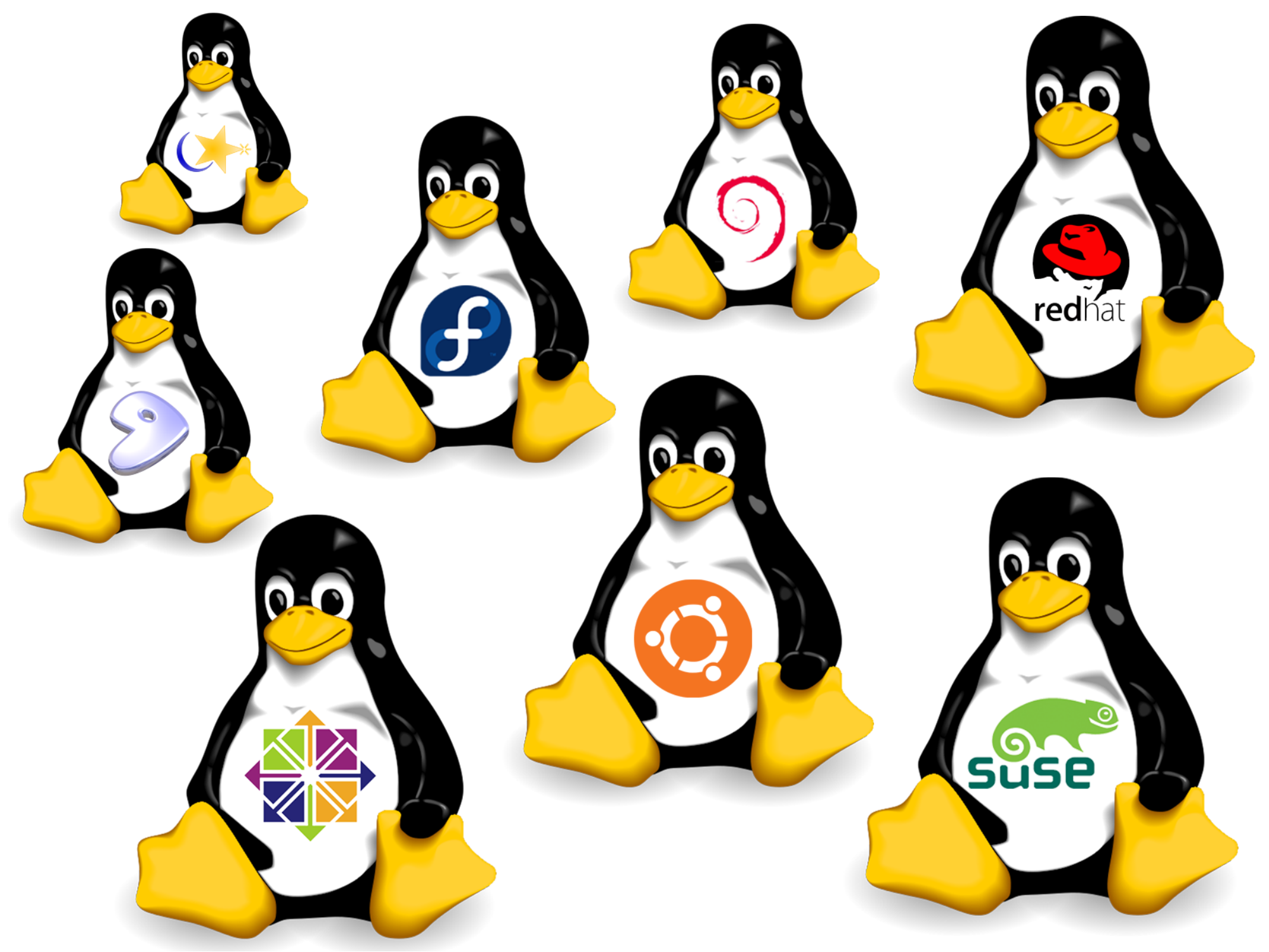
@corbett

Pasadena, CA, Physics Postdoc

All software is political. Technology shapes the course of our world and lines of code are votes for a particular future.

Working on Signal iOS, 2013


iPod
3:29
Tuesday, September 22
Signal 2m ago
New Message!
slide to view


redhat
suse

Author Photo © Norbert Schiller

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by *The Economist*. He is the author of twelve books—including his seminal work, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, and *Secrets & Lies: Digital Security in a Networked World* as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and blog "Schneier on Security" are read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc. You can read his blog, essays, and academic papers at www.schneier.com. He tweets at @schneierblog.

Praise for

APPLIED CRYPTOGRAPHY

"This book should be on the shelf of any computer professional involved in the use or implementation of cryptography."
— IEEE Software

"An encyclopedic survey … could well have been subtitled '*The Joy of Encrypting*' ... a useful addition to the library of any active or would-be security practitioner."
— Cryptologia

"…the best introduction to cryptography I've ever seen…The book the National Security Agency wanted never to be published…"
— Wired magazine

"…easily ranks as one of the most authoritative in its field…"
— PC magazine

"…monumental…fascinating…comprehensive…the definitive work on cryptography for computer programmers…"
— Dr. Dobb's journal

Cover Design: Wiley
Cover Painting: Mona Mark

WILEY

Also available as an e-book

Written by the world's most renowned security technologist this special Anniversary Edition celebrates 20 years for the most definitive reference on cryptography ever published, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*. Inside security enthusiasts will find a compelling introduction by author Bruce Schneider written specifically for this keepsake edition.

Included in this edition:

- **Exclusive forward by Bruce Schneier**
- **Ways to defeat the key escrow mechanism**
- **Encryption algorithms, including algorithms from the former Soviet Union and South Africa, and the RC4 stream cipher**
- **Protocols for digital signatures, authentication, secure elections, digital cash, and more**
- **Detailed information on key management and cryptographic implementations**

Programming/Security
$70.00 USA / $84.00 CAN

ISBN 978-1-119-09672-6
57000
9 781119 096726

SCHNEIER

APPLIED CRYPTOGRAPHY

20TH ANNIVERSARY EDITION

WILEY

20TH ANNIVERSARY EDITION

APPLIED CRYPTOGRAPHY

Protocols, Algorithms, and Source Code in C

BRUCE SCHNEIER

WILEY

This smart, relevant guide is a must for all those committed to computer and cyber security. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. This book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and keeping keys secure. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems.

CREDITS:

TREVP.
MOVIEM.

ILLUSTRATION
C. CORBETT

AS IMPLEMENTED IN EXISEMPIRE BY
MOVIEM.
C. CORBETT
F. JACOBS

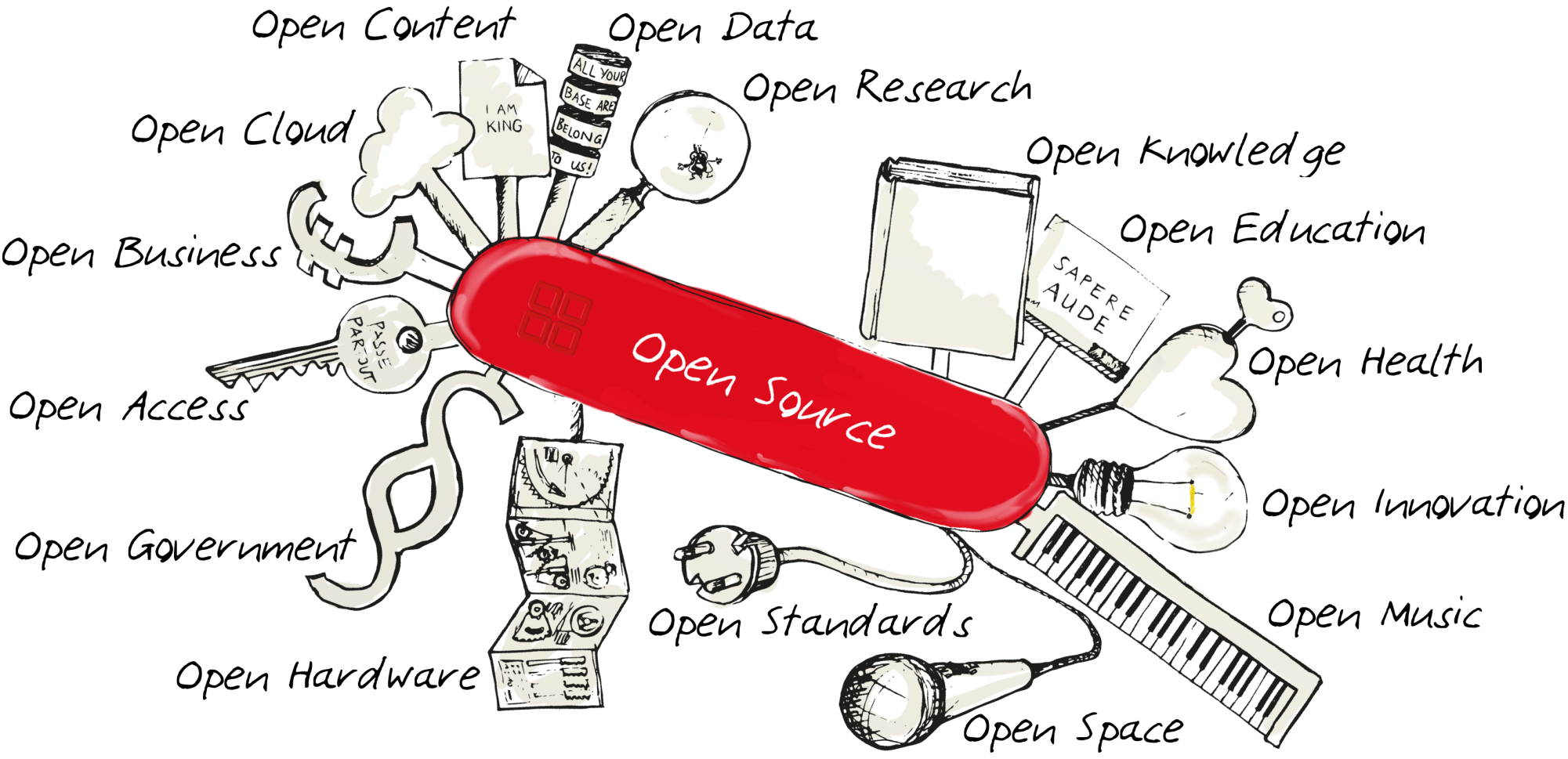
AXOLOTL PROTOCOL

AN ILLUSTRATED PRIMER


0040 86 d0 47 45 54 20 2f 6b 6c 69 71 2f 61 70 69 2f ..GET /k liq/api/
0050 67 69 76 65 5f 61 63 63 65 73 73 5f 74 6f 6b 65 give_acc ess_toke
0060 6e 2f 3f 61 63 63 65 73 73 5f 74 6f 6b 65 6e 3d n/?acces s_token=
0070 59 48 54 55 76 35 5f 71 58 4e 38 55 6c 56 45 69 YHTUv5_q XN8UlVEi

```
0040  e5 31 16 03 01 00 4a 02  00 00 46 03 01 4e 3a 5c   .1....J. ..F..N:\
0050  b6 28 6f b2 ab 44 39 bd  43 c8 74 ed f9 e7 d3 5c   .(o..D9. C.t....\
0060  b6 a3 ee cd 1f 8a c9 81  bc e4 b5 e0 ec 20 6c 53   ........ ..... lS
0070  95 ee f9 fd 83 18 7d f4  e9 14 7c 75 24 a2 d3 2e   ......}. ..|u$...
0080  4b 9a b5 1e 02 50 e9 be  da 24 0b 5c 5b d0 00 2f   K....P.. .$.\[../
0090  00 16 03 01 04 d9 0b 00  04 d5 00 04 d2 00 04 cf   ........ ........
00a0  30 82 04 cb 30 82 03 b3  a0 03 02 01 02 02 03 02   0...0... ........
00b0  a4 41 30 0d 06 09 2a 86  48 86 f7 0d 01 01 05 05   .A0...*. H.......
00c0  00 30 3c 31 0b 30 09 06  03 55 04 06 13 02 55 53   .0<1.0.. .U....US
00d0  31 17 30 15 06 03 55 04  0a 13 0e 47 65 6f 54 72   1.0...U. ...GeoTr
00e0  75 73 74 2c 20 49 6e 63  2e 31 14 30 12 06 03 55   ust, Inc .1.0...U
00f0  04 03 13 0b 52 61 70 69  64 53 53 4c 20 43 41 30   ....Rapi dSSL CA0
0100  1e 17 0d 31 31 30 38 30  31 31 37 32 30 32 38 5a   ...11080 1172028Z
0110  17 0d 31 32 30 38 30 33  31 39 30 30 31 32 5a 30   ..120803 190012Z0
0120  81 dd 31 29 30 27 06 03  55 04 05 13 20 4b 5a 6c   ..1)0'.. U... KZl
0130  6d 6e 31 76 6d 58 6c 32  57 4a 42 50 59 6a 73 6d   mn1vmXl2 WJBPYjsm
0140  33 4b 31 6e 44 38 49 79  6e 62 78 48 5a 31 0b 30   3K1nD8Iy nbxHZ1.0
0150  09 06 03 55 04 06 13 02  45 53 31 14 30 12 06 03   ...U.... ES1.0...
0160  55 04 0a 13 0b 77 77 77  2e 6b 6c 69 71 2e 69 6e   U....www .kliq.in
0170  31 13 30 11 06 03 55 04  0b 13 0a 47 54 30 38 39   1.0...U. ...GT089
```


php
MySQL
Perl
LINUX
python
APACHE
LAMP
Linux
Apache
MySQL
PHP,Perl,Python


Open Content
Open Data
Open Research
Open Cloud
Open Knowledge
Open Education
Open Business
Open Health
Open Access
Open Source
Open Innovation
Open Government
Open Standards
Open Music
Open Hardware
Open Space
I AM KING
ALL YOUR BASE ARE BELONG TO US!
SAPERE AUDE
PASSE PARTOUT


THE WIKILEAKS FILES
ALAIN BOMBARD
BOB CARR
Diary of a Foreign Minister
THE SPACE SHUTTLE OPERATOR'S MANUAL
90° South
Paul Sipple
THE EMPEROR FAR AWAY
DAVID EIMER
PETER GOLDSWORTHY
BUSHCRAFT 101
3M


250
200
150
100
50
25

@corbett

Pasadena, CA, Physics Postdoc

we need more people to participate in the technologcal “do-ocracy.” we cannot afford to gerrymander.

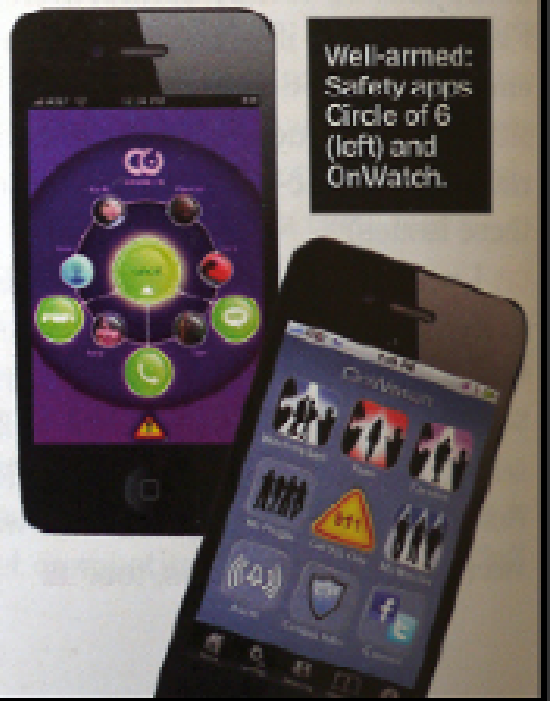
Working on Signal iOS, 2013

APPS THAT FIGHT RAPE

Move over, Mace, there's a new high-tech way to protect women from sexual violence

Unwilling to tolerate rampant sexual attacks in the Indian capital of Delhi, where one of every four rapes in the country occurs, a local nonprofit has devised an ingenious way to keep women safe: the "Fight Back" phone app. Acting as an SOS device, the program sends a text with the user's GPS location to up to five people, including the police, and as a post on Facebook and Twitter. "Even if the fear is that police are apathetic toward the problems of the people, your own friends and family will respond immediately," says Hindol Sengupta, cofounder of Whypoll, the "citizen networking" organization that designed the app.

For women in the U.S., the Department of Health and Human Services announced the development of two antiviolence apps: Circle of 6 will allow the user to alert six emergency contacts, and OnWatch will give women immediate access to 911 and campus police and dispatch their exact locations through GPS. Both are expected to be available as free downloads at the App Store in early 2012. —*Lauren N. Williams*

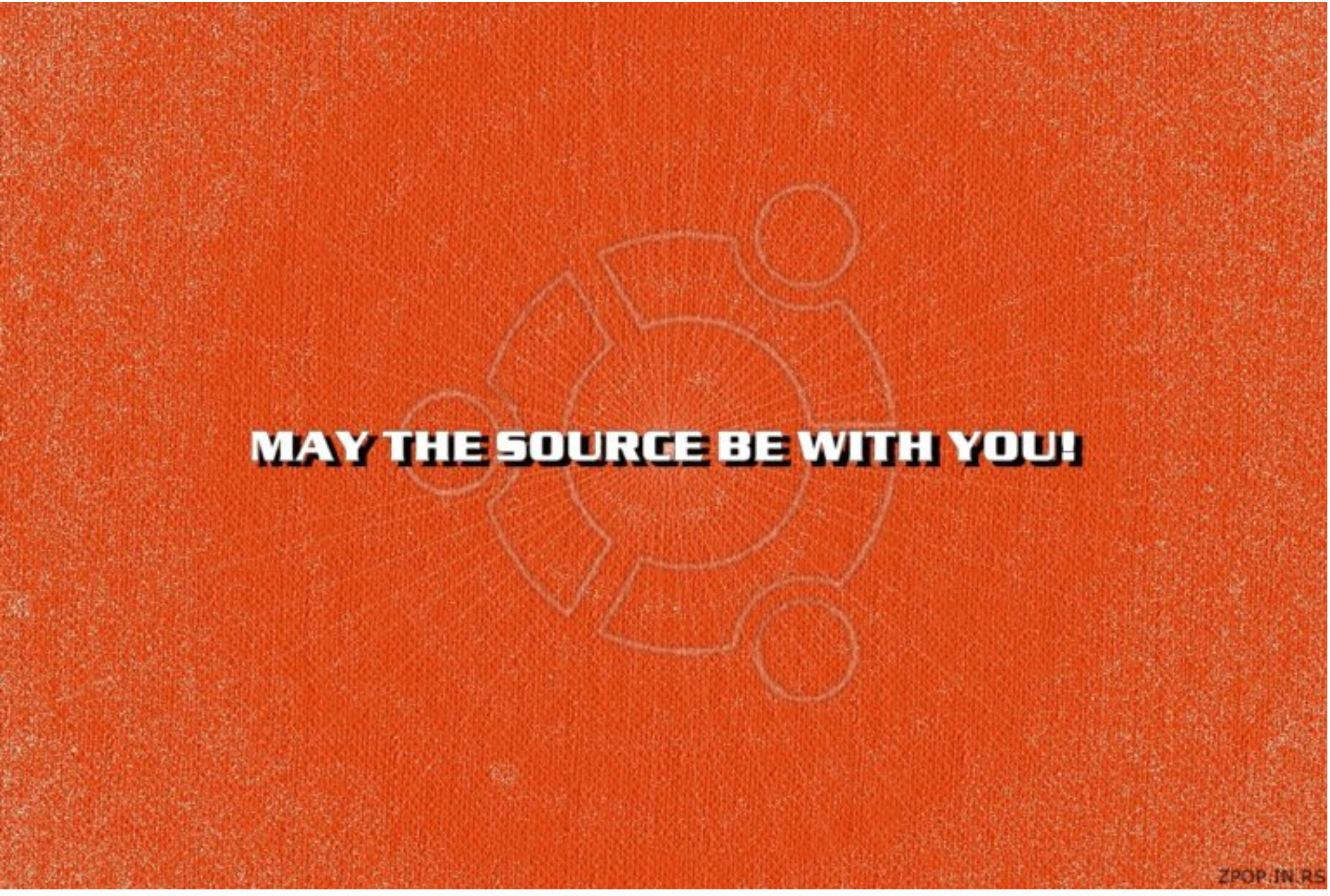


Well-armed: Safety apps Circle of 6 (left) and OnWatch.

A New App You Must Download Now

Called Circle of 6, this free app—it won first place in a contest sponsored by Vice President Joe Biden—helps you out of tricky social area and need a ride. Tap the car icon and a text goes out to six people you've previously chosen, asking for a lift and pulling your whereabouts from your phone's GPS. Or suppose you're desperate for a quick way out of talking to a creeper who's cornered you at a party. A tap on the phone icon asks the same six names for a phone call pretending they need you.

It's not for life-threatening scenarios; that's where 911 comes in.


MAY THE SOURCE BE WITH YOU!

@corbett

Pasadena, CA, Physics Postdoc

more evidence of #immigration turmoil in science: Prof unable to close hire of French Postdoc with Iranian heritage b/c they had other opt

4:34 PM - 3 Mar 2017

@corbett

Pasadena, CA, Physics Postdoc

more evidence of #immigration turmoil in science: postdoc at Caltech choosing to leave US for another job early b/c immigration uncertainty

4:34 PM - 3 Mar 2017

@corbett

Pasadena, CA, Physics Postdoc

Culture is more important than code, but code shapes culture.

November, 2016

@corbett

Pasadena, CA, Physics Postdoc

Choosing not to be political is not a choice everyone can make.

November, 2016

Purpose	OS X	Ubuntu
Edit text files	TextMate	Sublime
Organize Research papers	Papers.app	Mendeley
Resize windows on grid	SizeUp	CompizConfig Settings Manager
Site specific browser (standalone web apps)	Fluid	Google Chrome Shortcuts
Multiple desktops	Native	Unity tweak tool

@corbett

Pasadena, CA, Physics Postdoc

After being away for 1 year, so exciting to see how many more friends I can talk to on #Signal @whispersystems

1:34 PM - 6 Dec 2016

@corbett

Pasadena, CA, Physics Postdoc

We are in a post-truth society. If every scientist/engineer behaved like this? Truth is not a function of number of views. It exists.

1:29 AM - 9 Nov 2016

@corbett

Pasadena, CA, Physics Postdoc

I have not yet developed my position on @wikileaks. I have the cables, the internet, now where to start? where to finish?

5:31 AM - 4 Dec 2010

@corbett

Pasadena, CA, Physics Postdoc

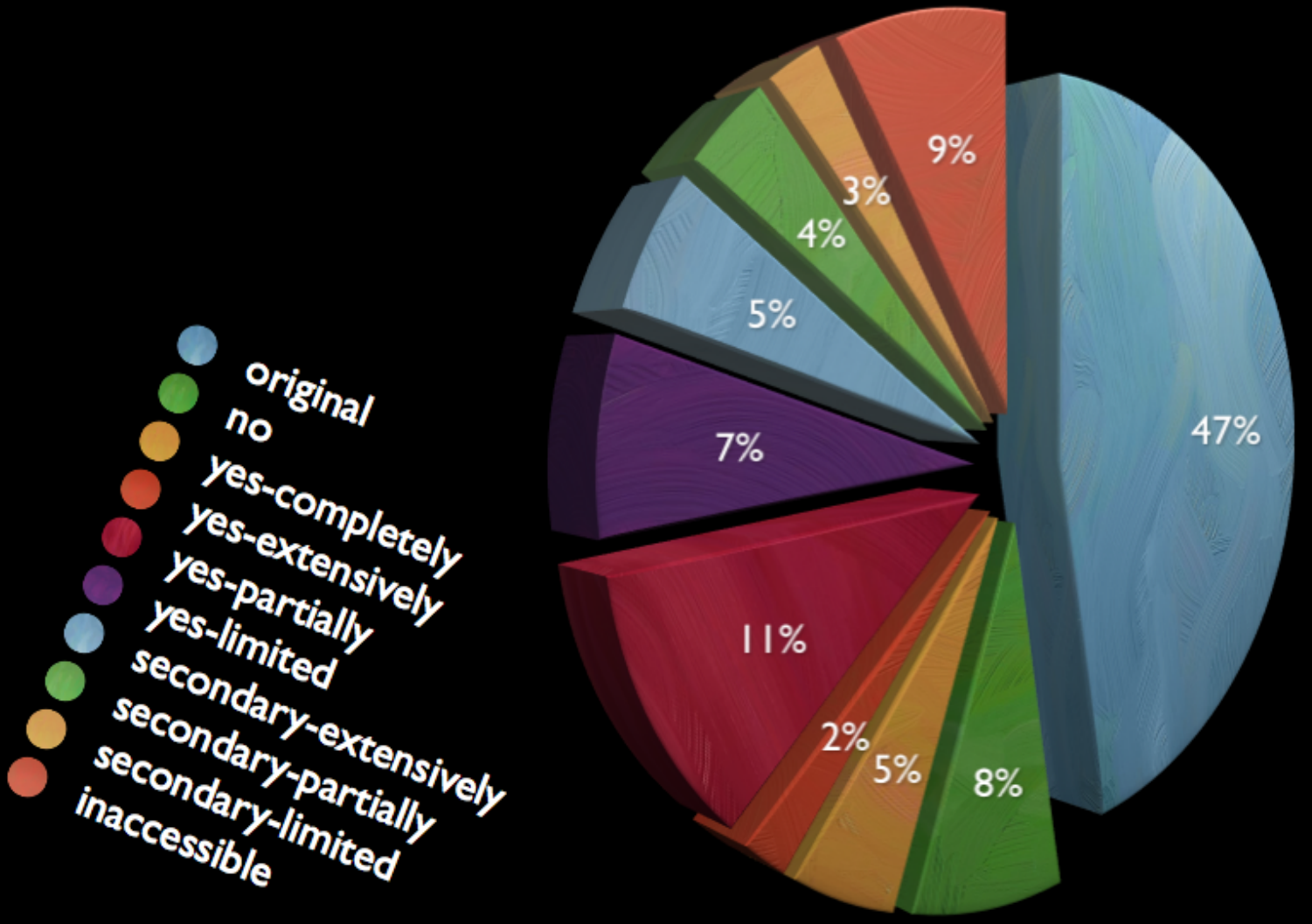
I like things thorough btw. before taking positions on Middle East affairs, I spent 4 years reading, studied Arabic, Hebrew, moved there 2x

5:33 AM - 4 Dec 2010

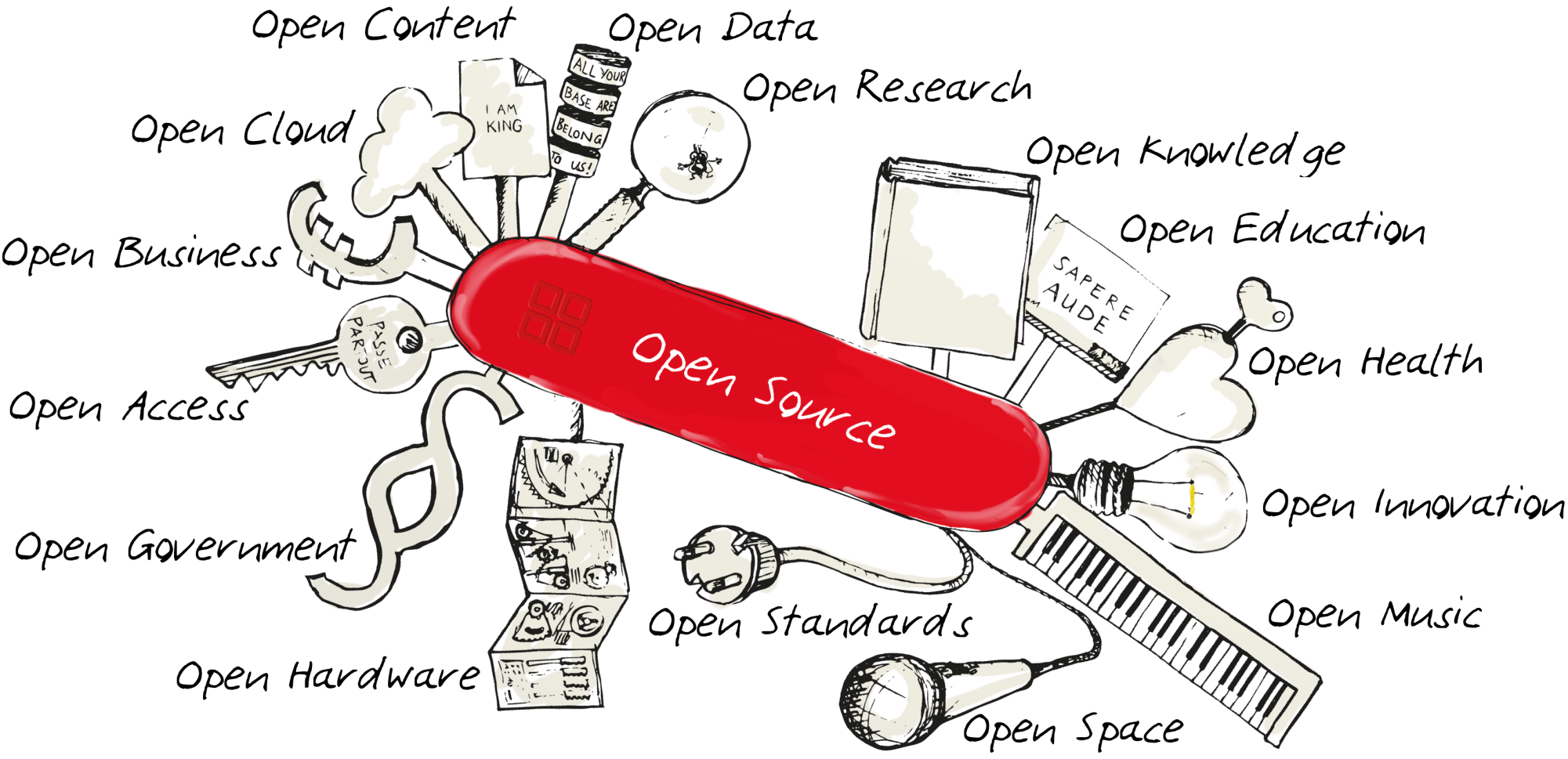
> A week ago I hatched a plan to educate myself in a more structured manner on what exactly Wikileaks stands for, its history, and its possible futures with the idea of developing a more concrete and informed opinion (and since I have a habit of taking action with respect to my opinions, thereby guiding my future actions). After seeking some advice about what to read via twitter and starting with this Julian Assange essay as a basis–a very good one for some philosophical background of the larger aims, I spent awhile digesting the Wikipedia page on Wikileaks before deciding I wanted to fact check its assertions and that its references might serve as a springboard the next step in my studies


138
136
315
186
133
316
311
180

The Numbers


original
no
yes-completely
yes-extensively
yes-partially
yes-limited
secondary-extensively
secondary-partially
secondary-limited
inaccessible
47%
8%
5%
2%
11%
7%
5%
4%
3%
9%


138
136
315
186
133
316
311
180


Open Content
Open Data
Open Research
Open Cloud
Open Knowledge
Open Education
Open Business
Open Health
Open Access
Open Source
Open Innovation
Open Government
Open Standards
Open Music
Open Hardware
Open Space
I AM KING
ALL YOUR BASE ARE BELONG TO US!
SAPERE AUDE
PASSE PARTOUT

@corbett

Pasadena, CA, Physics Postdoc

inclusive empowering in open source will positively shape our social landscape moving forward and change our political landscape

11:00 AM - 4 Mar 2017