

Security as a community healthcare: helping small non- profit organisations stay (slightly more) secure

Eva Blum-Dumontet
Researcher at Privacy International
eva@privacyinternational.org

PRIVACY INTERNATIONAL

- **Charity founded in 1990**
- **Based in London**
- **Defending privacy**
- **Fighting against corporate and government surveillance**

We learnt from our mistakes...



Home

Home Donate

Home

Because of known security vulnerabilities in Drupal we have taken the decision to reimplement our website from scratch. BRB

[Read more](#)

**We learn from the
organisations we work
with**

CODING
RIGHTS

TRANSLATING HUMAN RIGHTS
INTO CODES

TE
DIC.



Foundation for
Media Alternatives



OPEN DEMOCRACY
ADVICE CENTRE

TRANSPARENCY IN ACTION



www.7iber.com



DERECHOSDIGITALES

Derechos Humanos y Tecnología en América Latina

APC

Asociación por los Derechos Civiles



THE internet
CENTRE FOR & society



SMEX



RIGHT2KNOW



How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists

By *Ryan Gallagher*





Egyptian NGOs targeted in phishing campaign

BY JOE UCHILL - 02/02/17 10:56 AM EST

20 SHARES

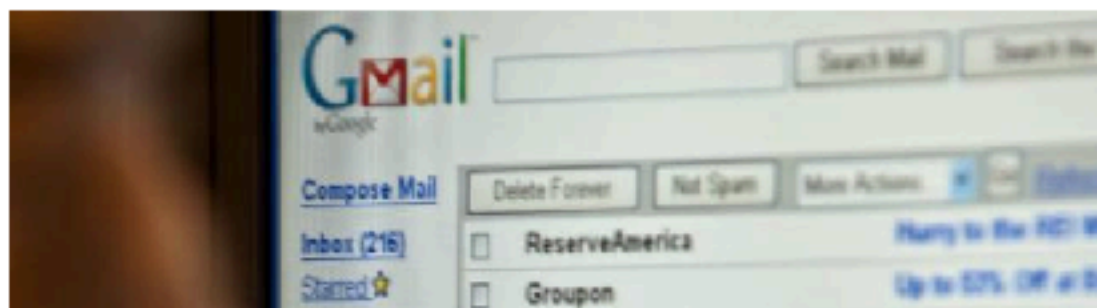


Just In...

Why consumer privacy laws should be de facto across America

OPINION — 36S AGO

Republican state senator in Kansas



Most Popular



GOP seeks separation from Trump on...

746 SHARES

26 Crónica | La Segunda jueves 26 octubre 2017

Mayores aportes provienen de fondos en Estados Unidos

Las platas extranjeras para defender el aborto y los derechos reproductivos

Fundación de Bill y Melinda Gates, así como de la escritora Isabel Allende, entre quienes hacen aportes.

Por Patricio Pino M.

El cálculo que el filántropo y fundador de Microsoft Bill Gates hizo en el diario británico «The Guardian» (el 13 de septiembre) es que US\$143 mil millones se destinan cada año a apoyar en todo el mundo a organizaciones dedicadas —entre otras cosas— a planificación familiar o derechos reproductivos, sea como actividades de difusión o investigación científica.

Desde hace tres décadas, una fracción de esas divisas llega a Chile. Y parte de esos aportes han sido recepcionados por organizaciones que alegaron ante el Tribunal Constitucional a favor del proyecto de interrupción del embarazo por tres causales.

La Bill & Melinda Gates Foundation está entre las que han enviado recursos.

dado en 1985, según el perfil en su web, el ICMER se dedica a estudiar la planificación familiar y salud sexual. Ese mismo perfil dice que han tenido apoyo de 10 donantes como la OMS, el Fondo de la ONU para la Población (UNFPA) y los Gates (en 2009 Bill dio US\$1,25 mil millones en ayuda por el mundo, entre ellos también US\$ 9 millones a la Diban). De todos ellos también es posible cuantificar el aporte del Wellcome Trust, fondo británico que en 1986 legó el magnate farmacéutico Henry Wellcome, que introdujo pastillas en Inglaterra.

Desde 2001 a la fecha la Asociación Chilena de Protección de la Familia (Aprofa) ha recibido en total US\$3,2 millones de la International Planned Parenthood Federation (IPPF), creada en 1952 y que en 2016 entregó US\$182 millones en todo el mundo. Aprofa la encabeza la ginecóloga Carmen Alvarado y en su directiva está Ramiro Molina, creador del Centro de Medicina Reproductiva y Desarrollo Integral del Adolescente (Cemera) de la U. de Chile. El año pasado IPPF recibió US\$130 millones en donativos: 60% de gobiernos (Suecia le dio US\$15 millones). La IPPF también ha

cabecera la chilena Lilian Sepúlveda.

Aunque en 30 años el Global Fund for Women, creado en 1987 en California, no suma US\$1 millón en donativos a seis organizaciones que actuaron ante el TC, sus aportes igual han sido amplios. En estas tres décadas ha ayudado a 90 organizaciones en Chile, sumando US\$2,6 millones. Entre ellas está la Corporación Humanas, encabezada por Carolina Carrera y en cuyo directorio está Kena Lorenzini, autora de un libro sobre Michelle Bachelet, miembro del Consejo Consultivo de Rompiendo el Silencio y hoy candidata al Senado por el Frente Amplio en la VII Región. Humanas alguna vez fue dirigida por Lorena Fries, actual subsecretaria de Derechos Humanos.

Con su sede en Sausalito (California), la Isabel Allende Foundation fue creada en 1995 por la escritora chilena en homenaje a

Global Fund
for Women

US\$ 731.000
a Fondo Alquimia



Sara Mandujano

Fondo
Alquimia

**Those stories reflect the diversity
of threats our partners are facing:
phishing attacks, sophisticated
spyware, burglary...**

**But we also learnt from
companies that really
should have known better....**

Don't be that guy!

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/14/2017, 4:12 AM

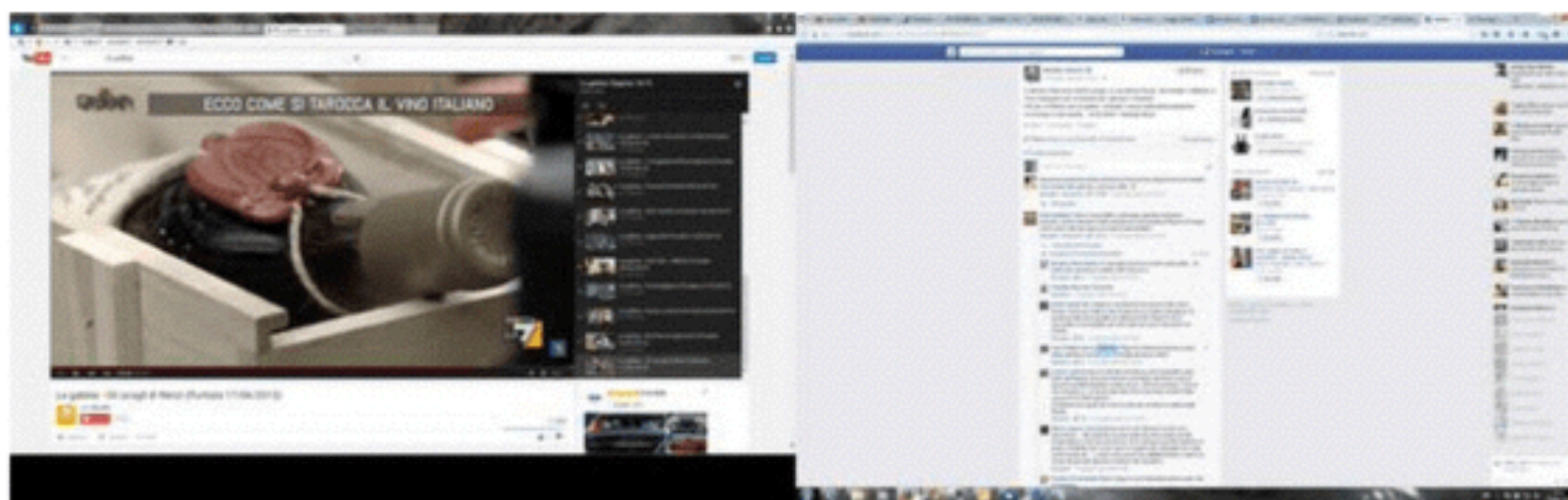


]HT[Hacked Team
@hackingteam



+ Follow

Our network security staff hard at work while 5 MB/s is transferred out of our internal network through his computer.



RETWEETS
23

FAVORITES
14



11:59 PM - 5 Jul 2015



What we found out when we audited our partner organisations

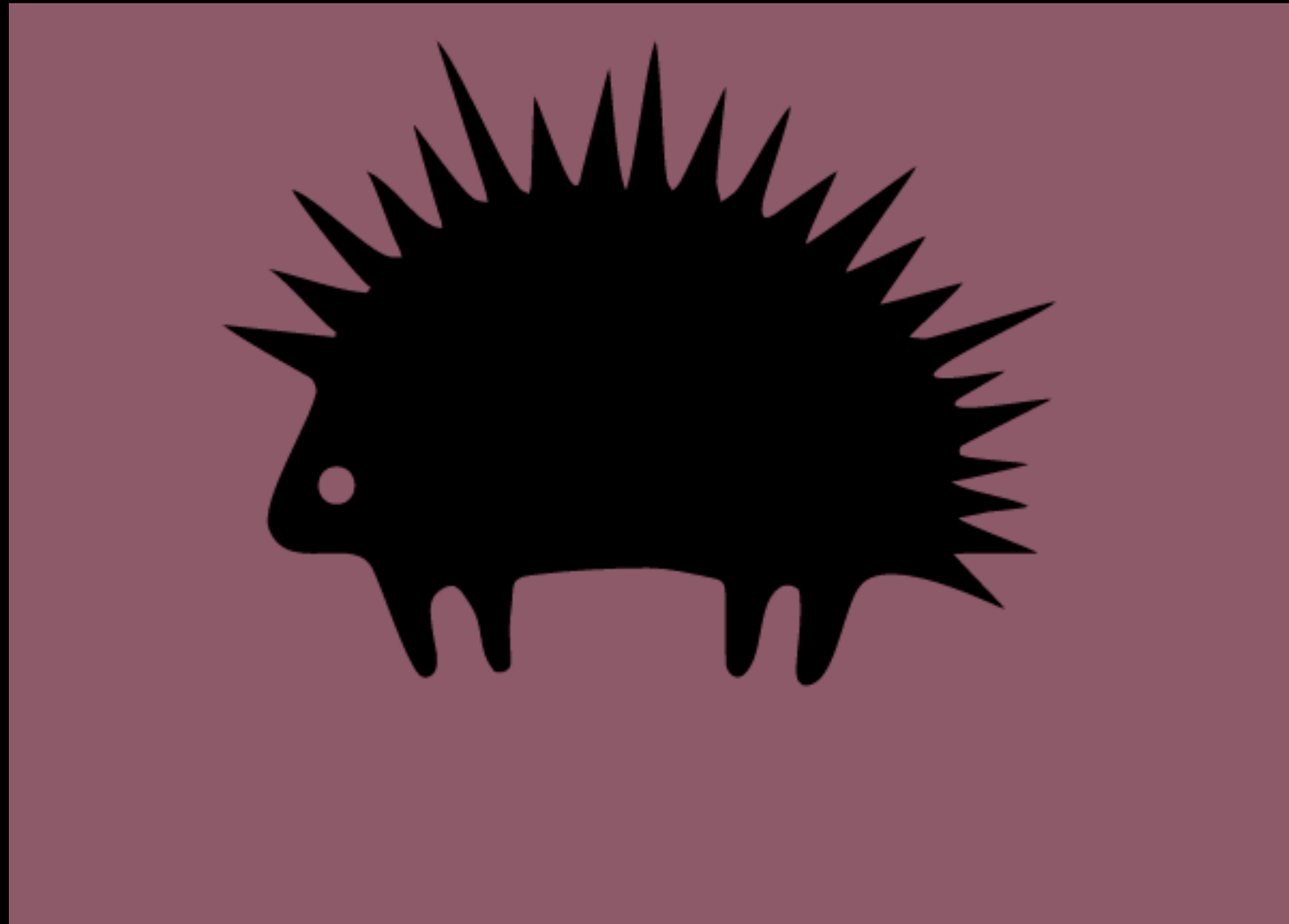
- Many of them relied on Google and US-based services in their organisations
- The security advice they had received so far was “use Signal, use Tor, use PGP, use strong passwords...” All focused on end-users.

**So instead of focusing on
end users we chose to
focus on the organisations**

**This is what led us to
think of security as a
community healthcare**

**When everyone is vaccinated, a contaminated person who comes in doesn't
harm the community**

This is how Thornsec was born!



So... What is Thornsec?

- A thorn in the sides of our adversaries by allowing organisations with little or no tech capability to run more secure fully-routed networks, with a strong set of firewall rules, and virtualisation of services.
- A network architecture described in a series of human-readable unit tests

Please go and look at our code!

<https://github.com/privacyint/thornsec-core>

What are we trying to
achieve with Thornsec?

Creating a secure network
where machines can't
communicate among
themselves

Bringing the responsibility of security back at the top

People at the very top should be the one held responsible when the data of 145 million US citizens get leaked because of a vulnerability that wasn't patched

Regaining control over our network



How much data has left your network since this morning? In the past year? What is “normal”?

Subject [eva.office] Daily Bandwidth Digest

11/09/2018, 07:25

UL: 13M
DL: 86M

=====

As you know, one of the key advantages afforded by operating our network through Thornsec is that it monitors for uploading traffic. The reason for this is that we want to try and check for any data exfiltration from our network.

Part of this monitoring allows our router to give you a daily digest of how much you've downloaded and uploaded.

This is not a punitive email, this information is not logged, and is only sent to you, as a user. This will hopefully alert you to any strange activity coming from your device.

If you think there is something suspicious about the figures above, please forward this email to the Tech Team so they can look into it for you.

Thanks!
Tech Team

Subject [eva.office] Upload bandwidth notification

29/05/2018, 12:40

To Me <eva@privacyinternational.org> ☆

As you know, one of the key advantages afforded by operating our network through Thornsec is that it monitors for uploading traffic. The reason for this is that we want to try and check for any data exfiltration from our network.

Our router has noticed that you have uploaded more than 20mb in a single connection. While this may be entirely normal for you, our router is set to identify this type of activity as a potential exfiltration. That is, it's possible your computer has been compromised and data is being uploaded to an external server. (Just ask Hacking Team about that!)

Over the next little while we are going to start speed-limiting uploads which are over 20mb, and will be alerting both you and the Tech Team every time this happens.

It is important to note a couple of things: as a privacy organisation, we aren't using this to snoop on what you're up to! However, we do have a lot of sensitive data inside our network, and we will be putting some precautions in place for large uploads.

We want this to be an inclusive feedback process so that we can try and minimise false positives before starting to roll out these precautions – if you've received this email and aren't doing anything you perceive to be out of the ordinary, please let us know.

You will only receive one of these email notices per hour.

Thanks!
Tech Team

Running our own services

We use Drupal, OwnCloud, Etherpad, Redmine...

Becoming accessible to all

That's the part we are still working on...

Thank you for listening!

- Thornsec: <https://github.com/privacyint/thornsec-core>
- eva@privacyinternational.org
- @Arcadian_O