

Broken

TRUST

[how soon
can we **re**boot?]

SECURITY AND PRIVACY



Protecting the intangible

Since 1989

TRUST  INFORMATICA

JULY 2013 WASHINGTON POST-ABC NEWS POLL - NATIONAL POLITICS, TRAYVON MARTIN, HEALTH CARE

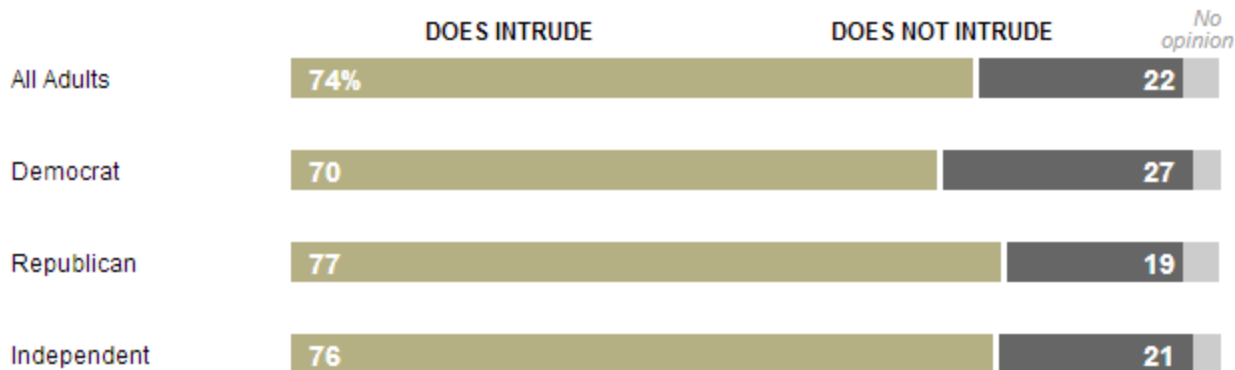
Q: Do you think that the National Security Agency's surveillance of telephone call records and internet traffic does or does not intrude on some Americans' privacy rights?

Published: July 26

Results by Party ID

Show results by:

Party ID



The Washington Post - ABC News poll



Protecting the intangible

Since 1989

TRUST  INFORMATICA



Protecting the intangible

Since 1989


TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA



SHIFT
FREEDOM



Since 1989

TRUST  INFORMATICA





TRUST  INFORMATICA



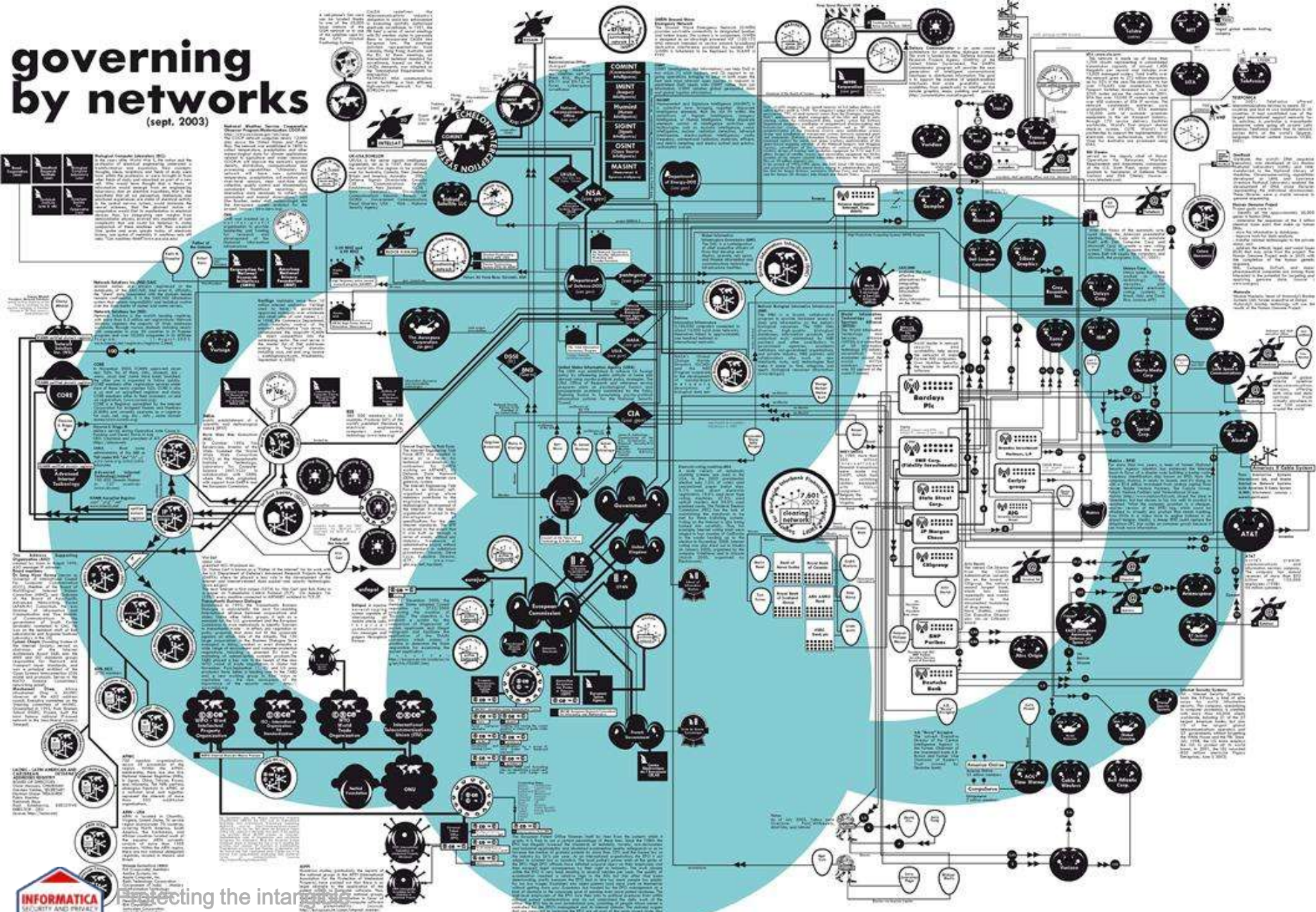
Protecting the intangible

Since 1989

TRUST  INFORMATICA

governing by networks

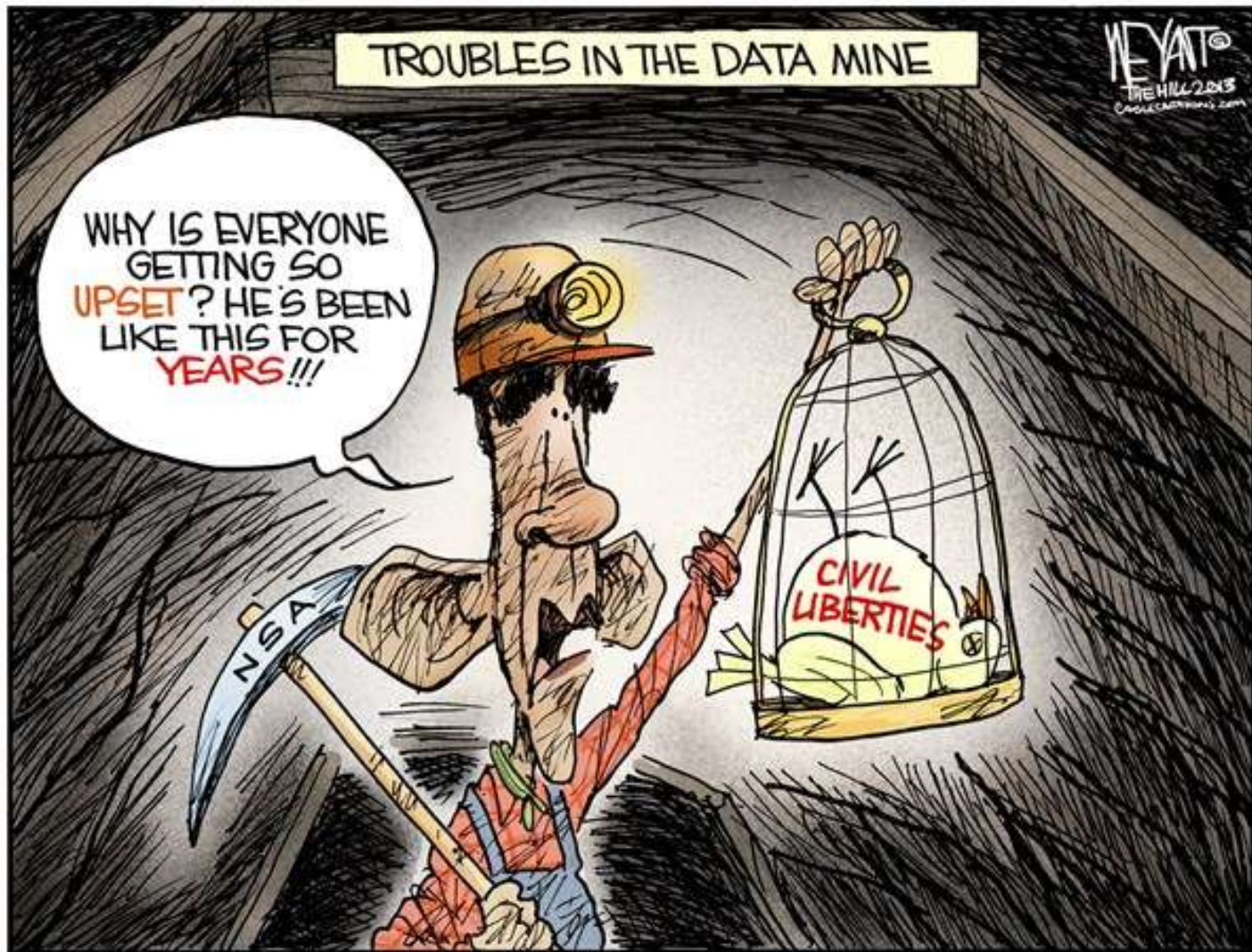
(sept. 2003)



Protecting the intangible

Since 1989

TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker and John Kelsey

**Computer Security Division
Information Technology Laboratory**

COMPUTER SECURITY



Protecting the intangible
Since 1989

TRUST  INFORMATICA



NIST



The Security Division of EMC



Protecting the intangible

Since 1989

TRUST  INFORMATICA



US008396213B2

(12) **United States Patent**
Brown et al.

(10) **Patent No.:** **US 8,396,213 B2**

(45) **Date of Patent:** **Mar. 12, 2013**

(54) **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

(75) Inventors: **Daniel R. L. Brown**, Mississauga (CA);
Scott A. Vanstone, Campbellville (CA)

(73) Assignee: **Certicom Corp.**, Mississauga, Ontario (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1283 days.

(21) Appl. No.: **11/336,814**

(22) Filed: **Jan. 23, 2006**

(65) **Prior Publication Data**

US 2007/0189527 A1 Aug. 16, 2007

Related U.S. Application Data

(60) Provisional application No. 60/644,982, filed on Jan. 21, 2005.

(51) **Int. Cl.** (2006.01)
H04L 9/00

(52) **U.S. Cl.** 380/44; 380/286; 380/28; 380/45; 380/46; 713/157

(58) **Field of Classification Search** 380/20-30, 380/44-47, 277-286; 713/170-171
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,442,707 A * 8/1995 Miyaji et al. 380/30
6,044,388 A * 3/2000 DeBellis et al. 708/254
6,088,798 A * 7/2000 Shimbo 713/176
6,243,467 B1 * 6/2001 Reiter et al. 380/30
6,263,081 B1 * 7/2001 Miyaji et al. 380/28
6,307,935 B1 * 10/2001 Crandall et al. 380/28

6,424,712 B2 * 7/2002 Vanstone et al. 380/28
6,477,254 B1 * 11/2002 Miyazaki et al. 380/286
6,714,648 B2 * 3/2004 Miyazaki et al. 380/30
6,738,478 B1 * 5/2004 Vanstone et al. 380/28
6,882,958 B2 * 4/2005 Schmidt et al. 702/179
7,013,047 B2 * 3/2006 Schmidt et al. 382/199
7,062,043 B1 * 6/2006 Solinas 380/30
7,062,044 B1 * 6/2006 Solinas 380/30

(Continued)

FOREIGN PATENT DOCUMENTS

CA 2381397 A1 2/2001
JP 2001222220 8/2001

(Continued)

OTHER PUBLICATIONS

Dr RW Lichota, Verifying the correctness of cryptographic proofs using "convince", IEEE, Dec. 13, 1996, pp. 119-122.*

(Continued)

Primary Examiner — Nathan Flynn

Assistant Examiner — Viral Lakhia

(74) *Attorney, Agent, or Firm* — Fish & Richardson P.C.

(57) **ABSTRACT**

An elliptic curve random number generator avoids escrow keys by choosing a point Q on the elliptic curve as verifiably random. An arbitrary string is chosen and a hash of that string computed. The hash is then converted to a field element of the desired field, the field element regarded as the x-coordinate of a point Q on the elliptic curve and the x-coordinate is tested for validity on the desired elliptic curve. If valid, the x-coordinate is decompressed to the point Q, wherein the choice of which is the two points is also derived from the hash value. Intentional use of escrow keys can provide for back up functionality. The relationship between P and Q is used as an escrow key and stored by for a security domain. The administrator logs the output of the generator to reconstruct the random number with the escrow key.

64 Claims, 6 Drawing Sheets



Protecting the intangible

Since 1989

TRUST  INFORMATICA

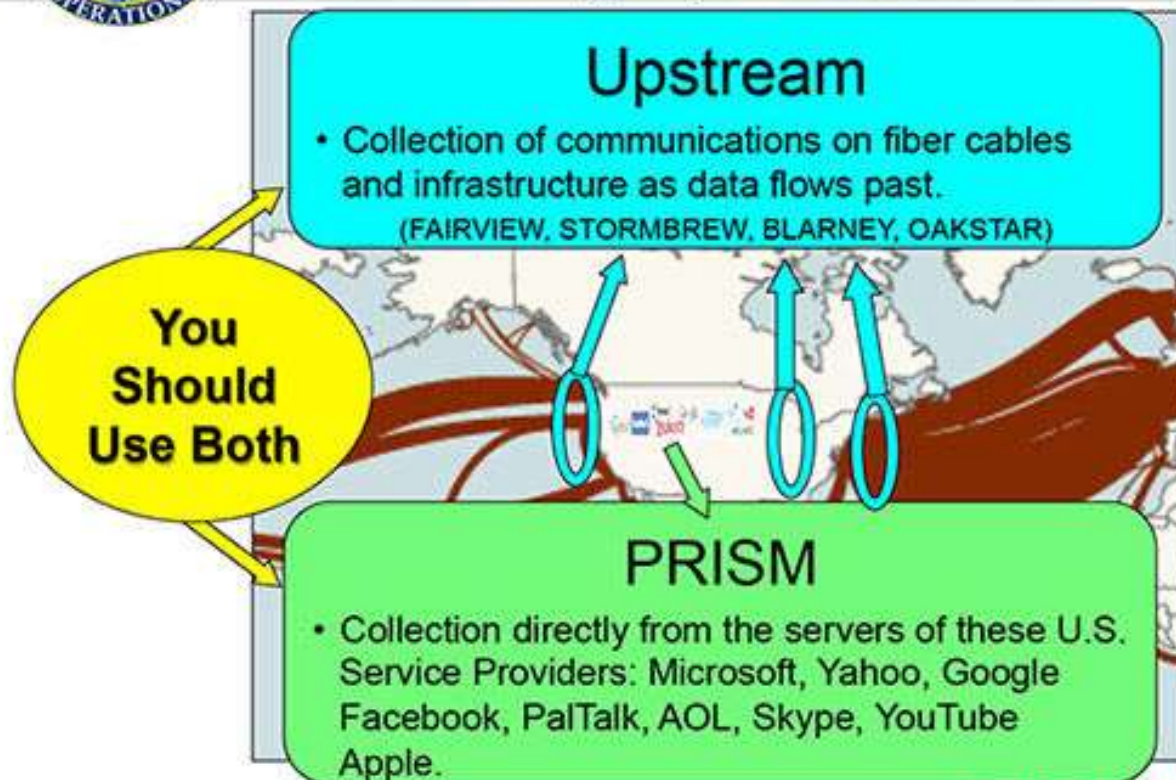


Protecting the intangible
Since 1989

TRUST  INFORMATICA



(TS//SI//NF) **FAA702 Operations**
Two Types of Collection



TOP SECRET//SI//ORCON//NOFORN

See the entire collection of published NSA slides ›

U.S. cloud industry stands to lose \$35 billion amid PRISM fallout

Summary: Revelations of the U.S. government's spying programs could have a massive impact on the U.S. cloud industry, which stands to lose vast sums over the next three years as a result — compounded by other countries bankrolling efforts to combat U.S. market leadership.



By Zack Whittaker for Zero Day | August 6, 2013 -- 09:16 GMT (02:16 PDT)

Follow @zackwhittaker



Protecting the intangible

Since 1989

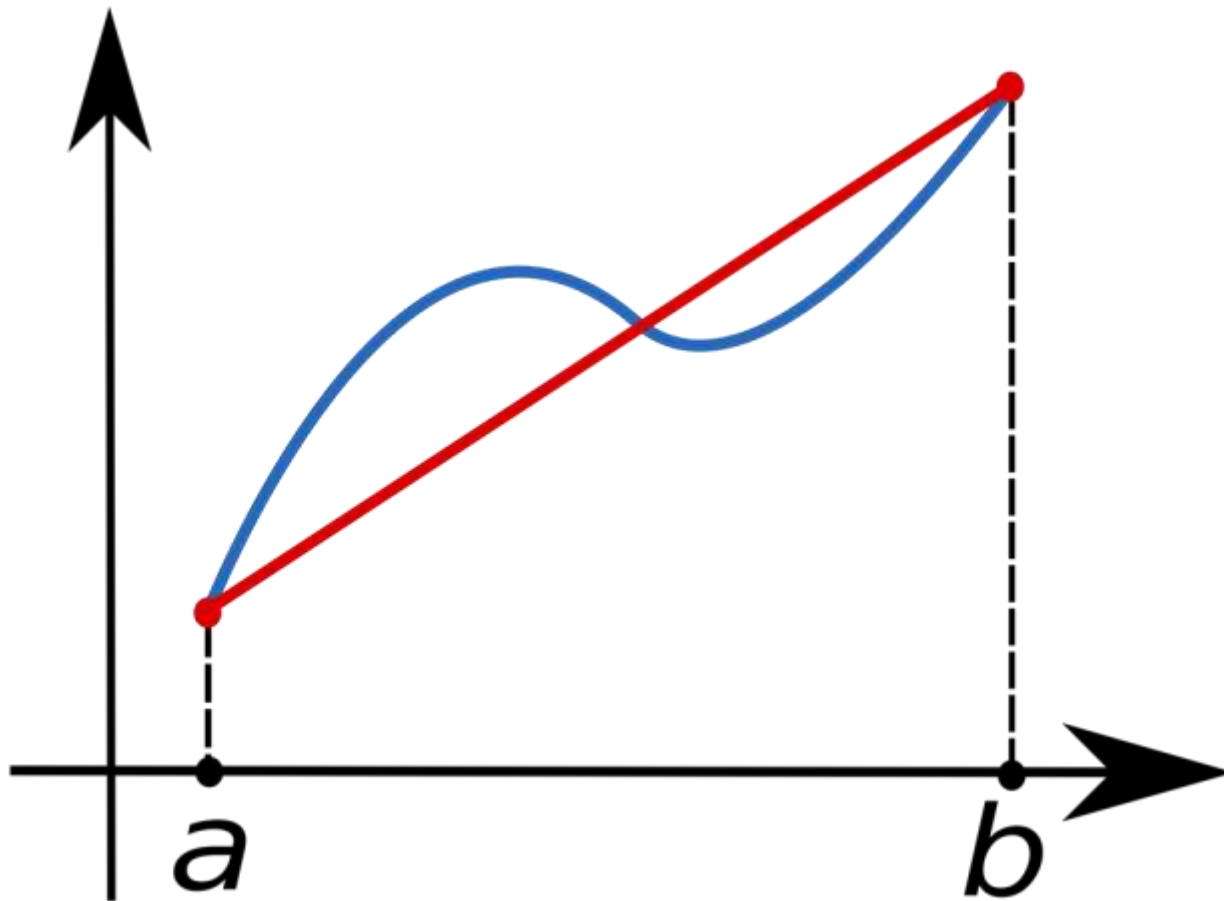
TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA





Protecting the intangible

Since 1989

TRUST  INFORMATICA

The FBI has not been here

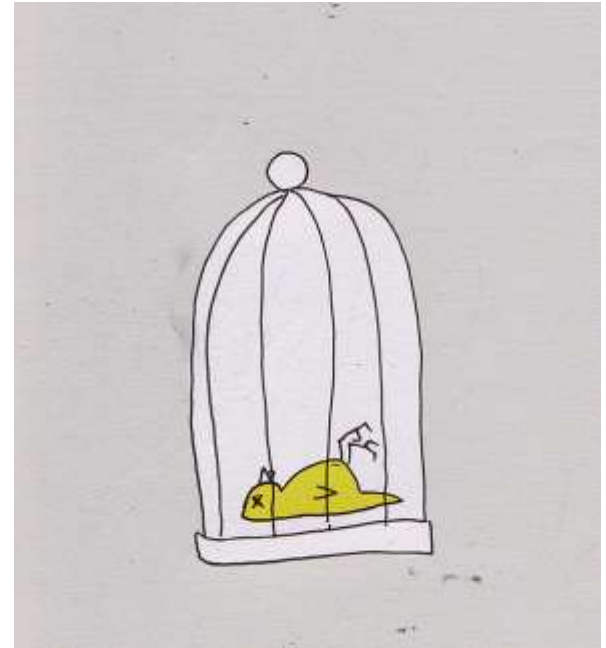
[watch very closely for the removal of this sign]



Protecting the intangible

Since 1989

TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA

In Remarkable Turnaround, Republicans Officially Denounce NSA Phone Surveillance

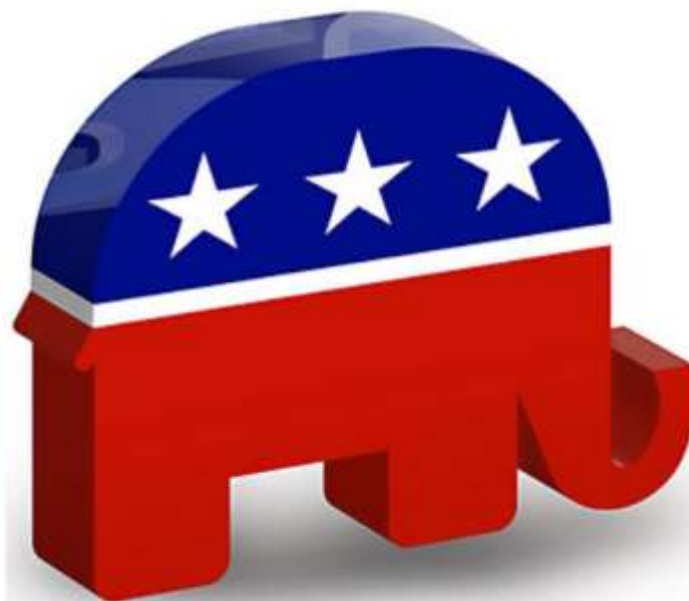
—By **Kevin Drum** | Sat Jan. 25, 2014 9:21 AM GMT

439 Tweet 237 Like 6.4k

This is easily the most remarkable story of the year so far. As you read it, keep in mind that this is not about a resolution from some fringe libertarian group. It's about a resolution from the Republican National Committee, the very embodiment of establishment conservatism:

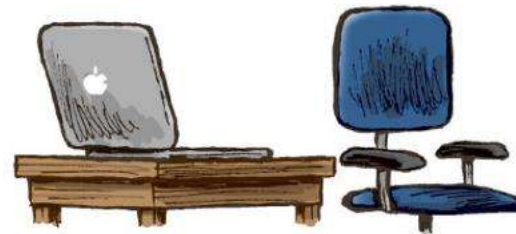
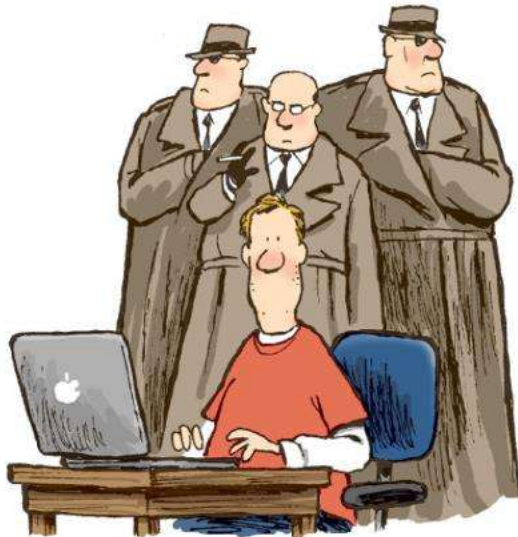
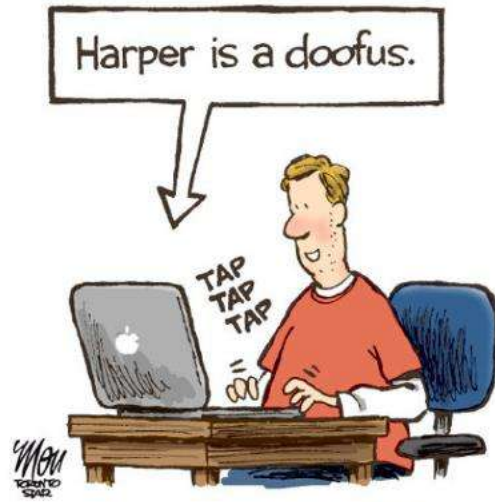
In a jarring break from the George W. Bush era, the Republican National Committee voted Friday to adopt a resolution demanding an investigation into the National Security Agency's spy programs.

According to the resolution, the NSA metadata program revealed by former NSA contractor Edward Snowden is deemed "an invasion



Protecting the intangible
Since 1989

TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA



Protecting the intangible
Since 1989

TRUST  INFORMATICA



Is TrueCrypt Audited Yet? **Not Yet.**

Snowden: AES is safe



Protecting the intangible

Since 1989

TRUST  INFORMATICA



Protecting the intangible

Since 1989

TRUST  INFORMATICA



ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

OCTOBER 25, 2013 | BY **DANNY O'BRIEN**



Ten Steps You Can Take Right Now Against Internet Surveillance

One of the trends we've seen is how, as the word of the NSA's spying has spread, more and more ordinary people want to know how (or if) they can defend themselves from surveillance online. But where to start?

The bad news is: if you're being personally targeted by a powerful intelligence agency like the NSA, it's very, very difficult to defend yourself. The good news, if you can call it that, is that much of what the NSA is doing is mass surveillance on everybody. With a few small steps, you can make that kind of surveillance a lot more difficult and expensive, both against you individually, and more generally against everyone.



Protecting the intangible

Since 1989

TRUST  INFORMATICA

Where does this leave us?

- Bipartisan opposition
- Open source adoption
- Independent auditing
- Mistakes measurable
- Improved public awareness
- Reboot time: now
- Remediation time: just start





Follow
Read
Connect

[@infosuperjunkie](#) for smart, irreverent fun
[Subscribe.SecurityandPrivacy.ca](#) for blogs
[LinkedIn](#) | [Facebook](#) | [Google+](#) because you can