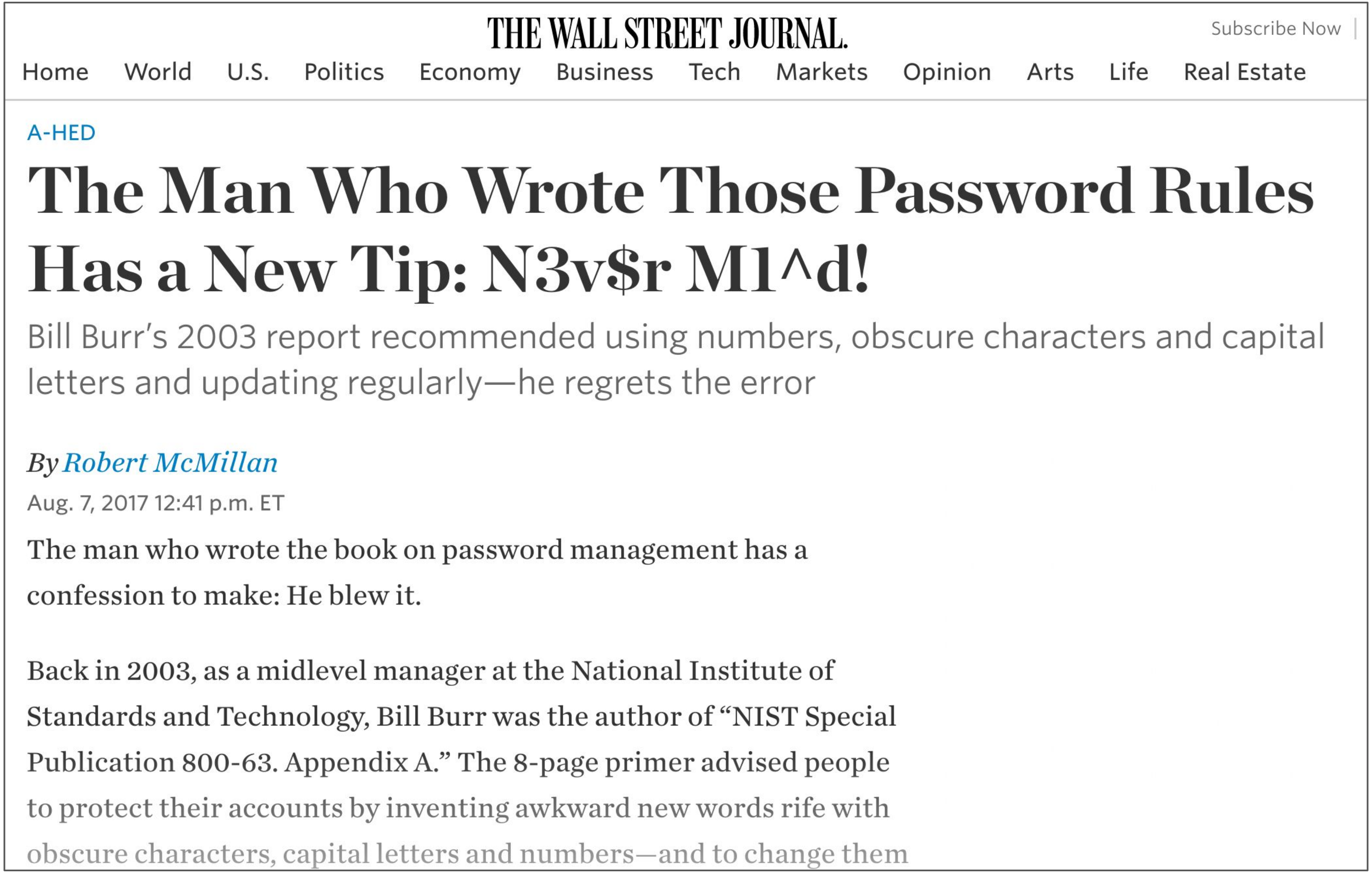
Passwords, Two Factor Authentication, HTTPS, Third Parties

in 10 minutes somehow

Eric Mill
Twitter: @konklone
Email: eric@konklone.com

You, each of you, need to use strong passwords

You, each of you, need to use a password manager



THE WALL STREET JOURNAL.

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

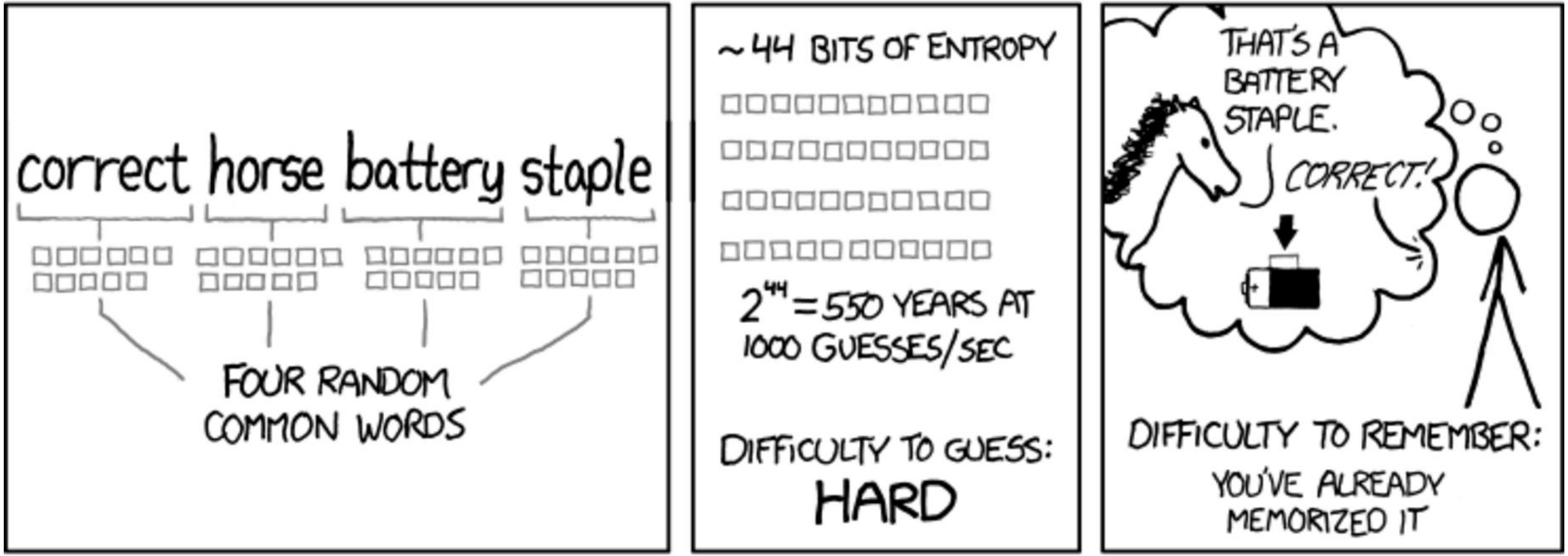
By Robert McMillan

Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of "NIST Special Publication 800-63. Appendix A." The 8-page primer advised people to protect their accounts by inventing awkward new words rife with obscure characters, capital letters and numbers—and to change them

Memorizing strong passphrases


correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

- **Password managers prevent password reuse**, which lets attackers grab passwords from a random web forum and then break into Amazon or Google accounts.

- Even though passphrases are much easier to memorize and don’t need to be rotated, **you still need unique secrets per-account**. And memorizing hundreds of these is impossible.

Ideal:

- memorized strong passphrase protecting all other passwords, with auto-fill in the browser

In practice:

- as close to that as is reasonable for you

Two factor authentication

- On top of a password, also something you **have** (or something you are, or...)

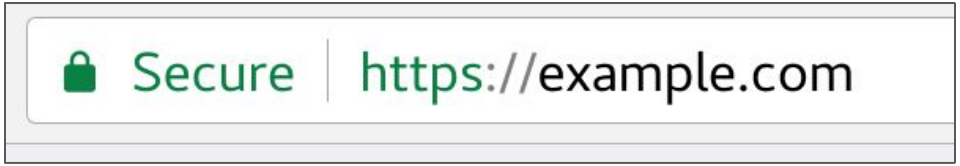
- SMS isn’t great at “something you have”, but **any second factor** is better than none

- Whenever possible, use non-SMS methods, especially...

Universal 2nd Factor (U2F)

Not just simple: also **seriously resists phishing** by only working when you're at the **right domain name**

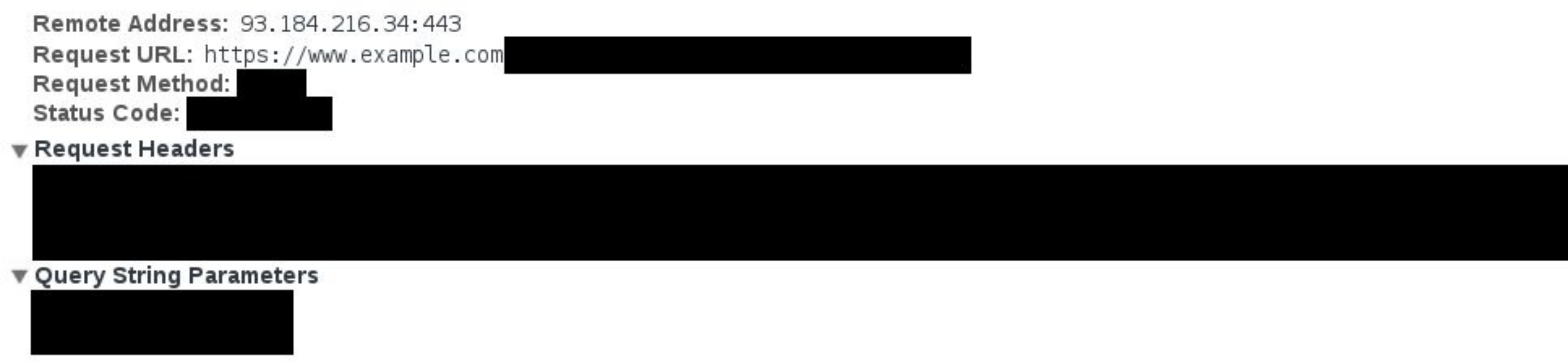
HTTPS



🔒 Secure | https://example.com

It actually does a pretty amazing job

Confidentiality (Privacy)



Remote Address: 93.184.216.34:443
Request URL: https://www.example.com[redacted]
Request Method: [redacted]
Status Code: [redacted]

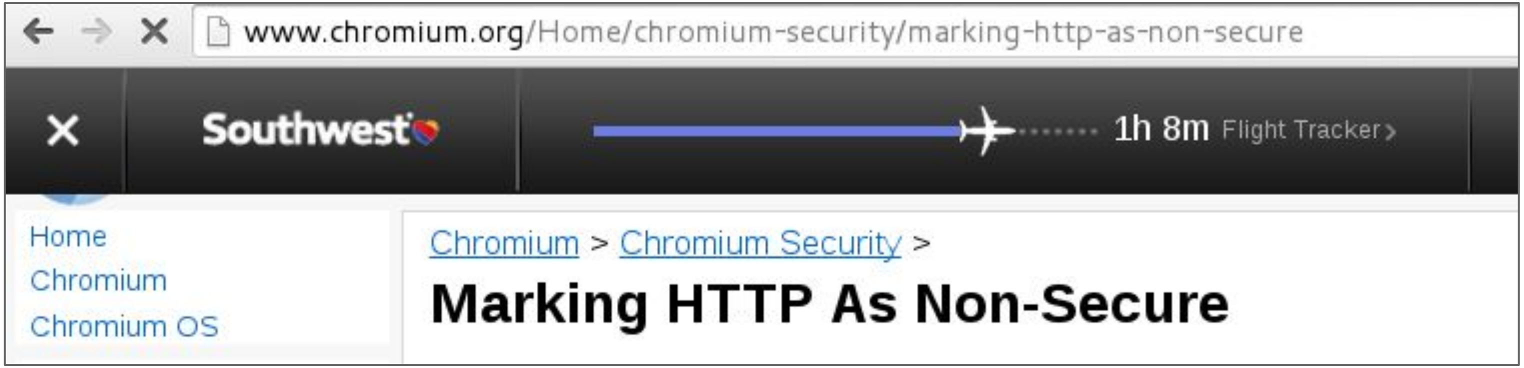
▼ **Request Headers**

[redacted]

▼ **Query String Parameters**

[redacted]

Integrity (Untouched)

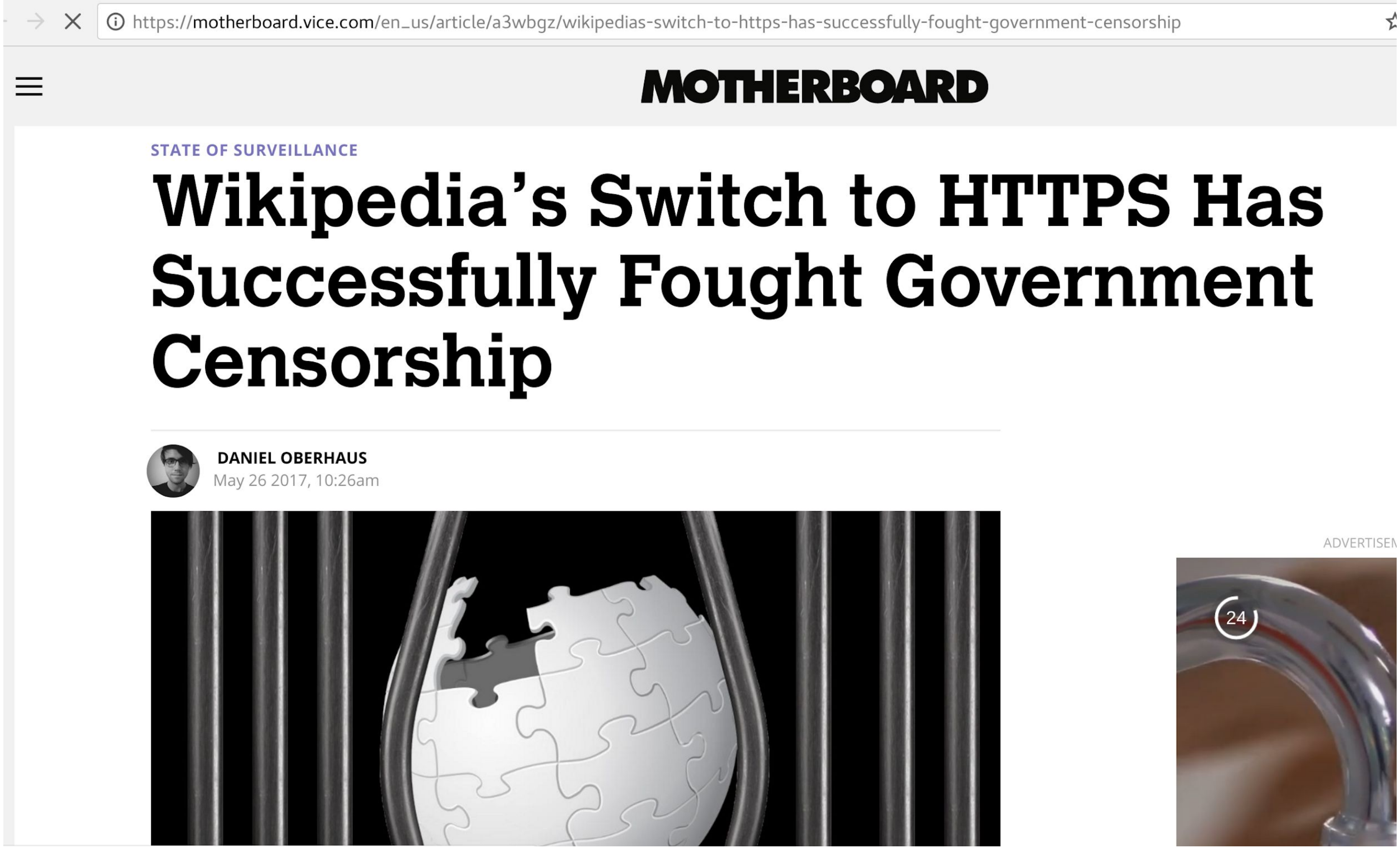


www.chromium.org/Home/chromium-security/marking-http-as-non-secure

Home
Chromium
Chromium OS

Chromium > Chromium Security >

Marking HTTP As Non-Secure



https://motherboard.vice.com/en_us/article/a3wbgz/wikipedias-switch-to-https-has-successfully-fought-government-censorship

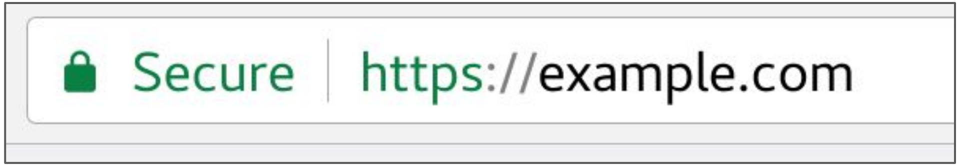
MOTHERBOARD

STATE OF SURVEILLANCE

Wikipedia’s Switch to HTTPS Has Successfully Fought Government Censorship

DANIEL OBERHAUS
May 26 2017, 10:26am

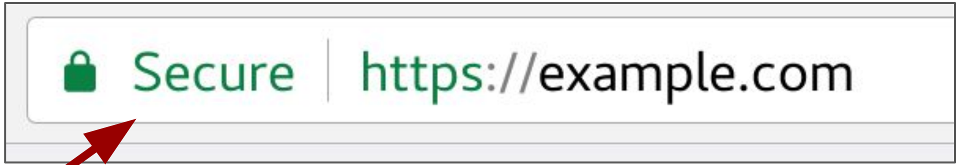
HTTPS



Secure https://example.com

Privacy, security, anti-censorship (but not anonymity)

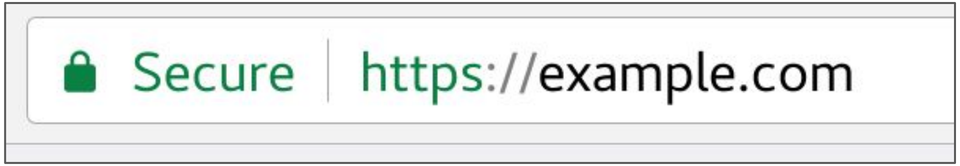
HTTPS



🔒 Secure | https://example.com

Only securing the connection. You can still be phished over HTTPS.

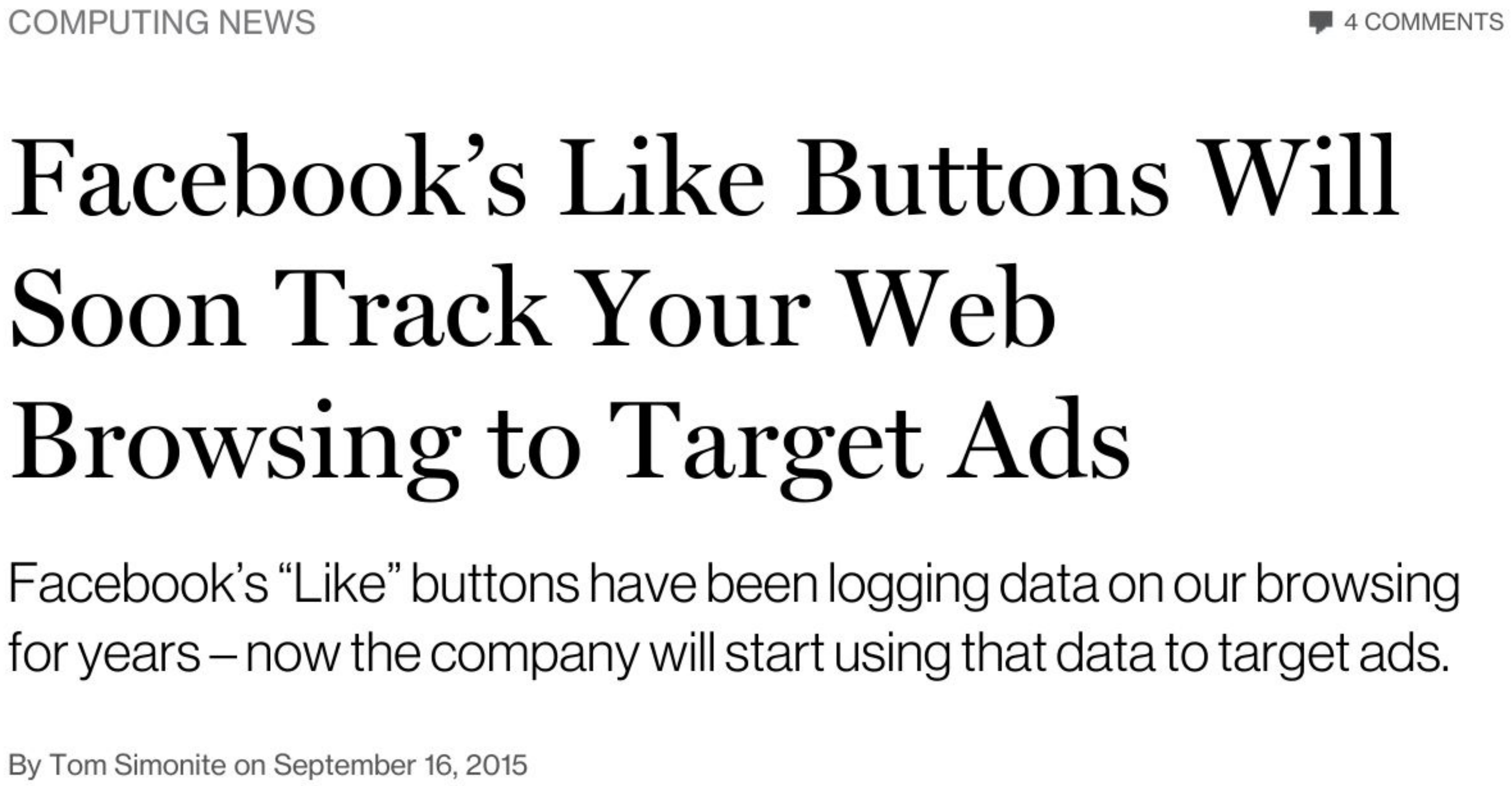
HTTPS



Secure | https://example.com

Strong protection,
even from governments,
even on a very hostile network.

Ads and third parties



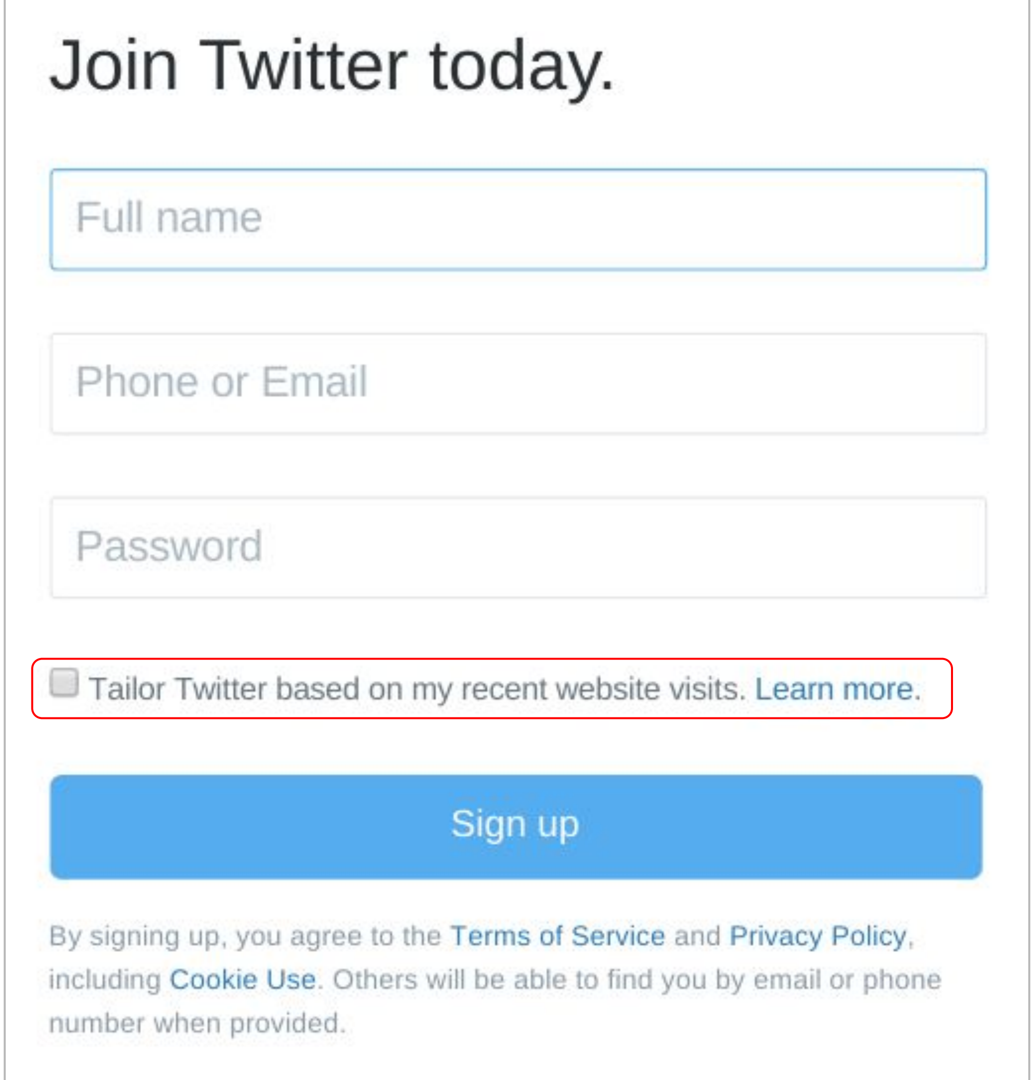
COMPUTING NEWS

4 COMMENTS

Facebook’s Like Buttons Will Soon Track Your Web Browsing to Target Ads

Facebook’s “Like” buttons have been logging data on our browsing for years – now the company will start using that data to target ads.

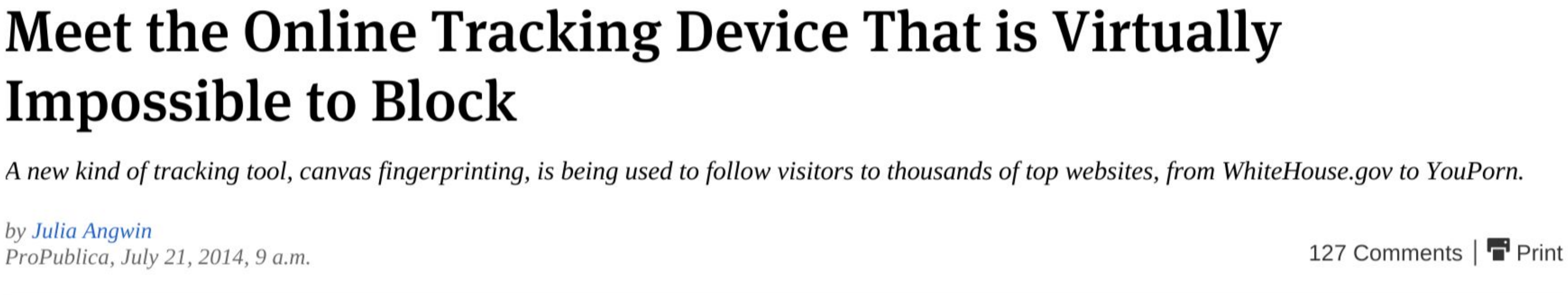
By Tom Simonite on September 16, 2015



Join Twitter today.

☐ Tailor Twitter based on my recent website visits. Learn more.

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use. Others will be able to find you by email or phone number when provided.



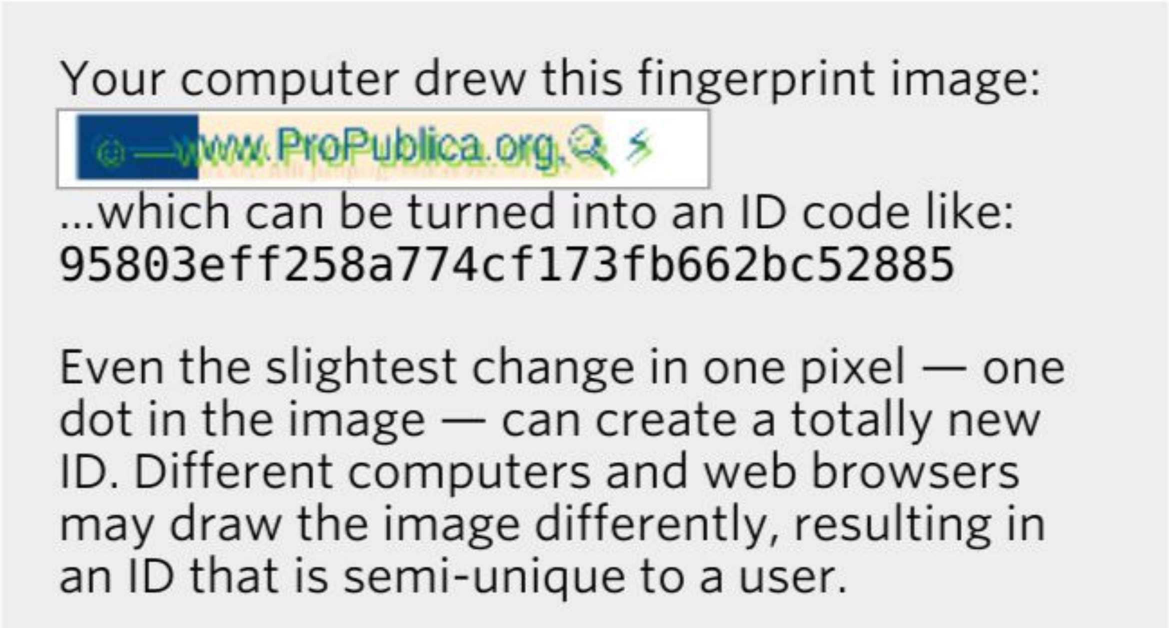
Meet the Online Tracking Device That is Virtually Impossible to Block

A new kind of tracking tool, canvas fingerprinting, is being used to follow visitors to thousands of top websites, from WhiteHouse.gov to YouPorn.

by Julia Angwin
ProPublica, July 21, 2014, 9 a.m.

127 Comments | Print

What "AddThis" Did



Your computer drew this fingerprint image:

...which can be turned into an ID code like:
95803eff258a774cf173fb662bc52885

Even the slightest change in one pixel — one dot in the image — can create a totally new ID. Different computers and web browsers may draw the image differently, resulting in an ID that is semi-unique to a user.

Passwords, Two Factor Authentication, HTTPS, Third Parties

in 10 minutes somehow

Eric Mill
Twitter: @konklone
Email: eric@konklone.com