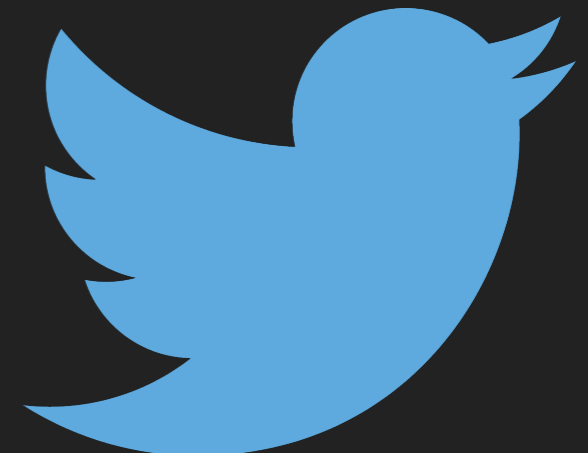


JOHN ADAMS

BEYOND FBI VS. APPLE

WHAT'S NEXT IN THE CRYPTO WARS?

INTRODUCTION – WHO AM I?



Disclaimer: These words are my own. I do not speak for these companies.

1977

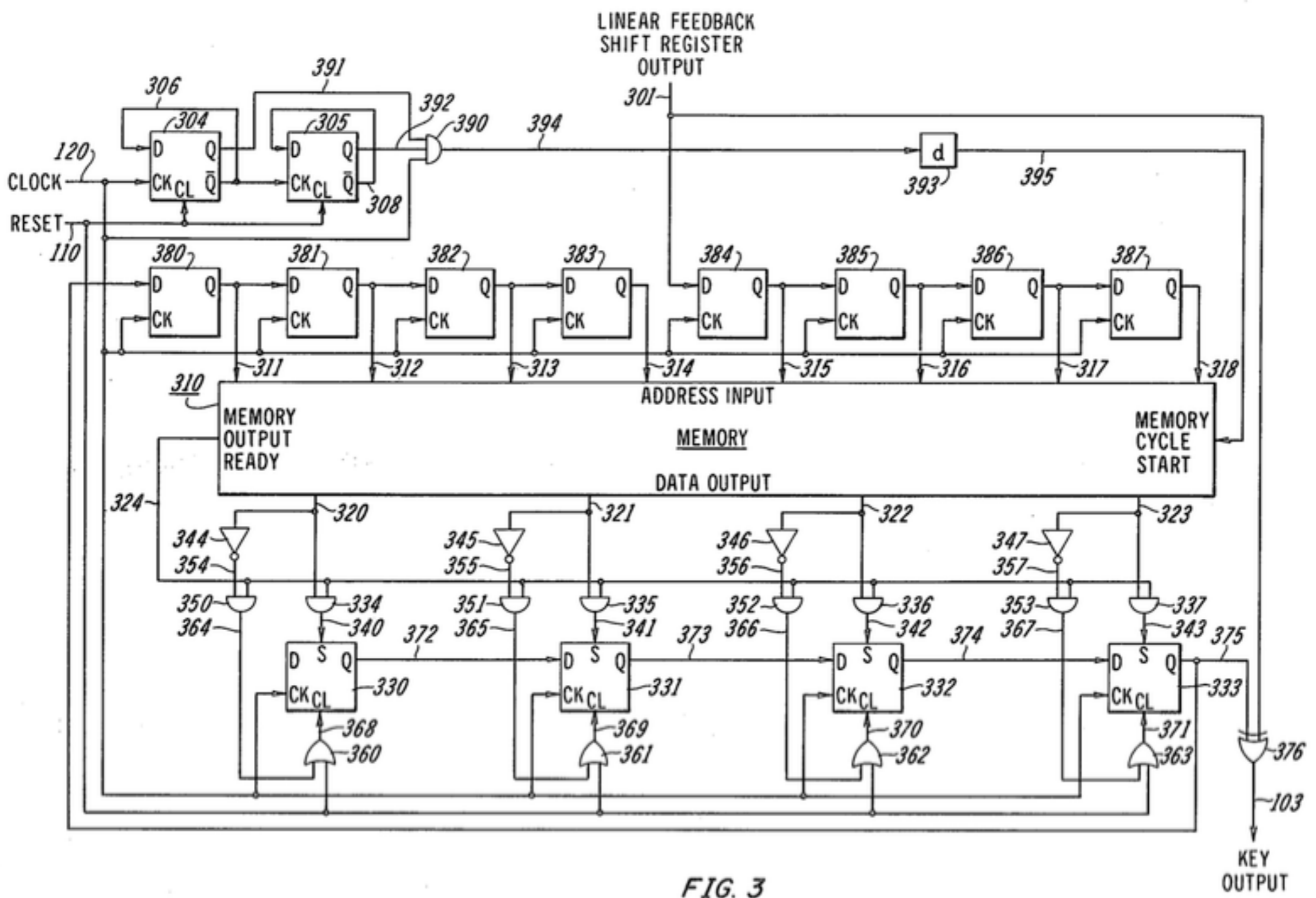
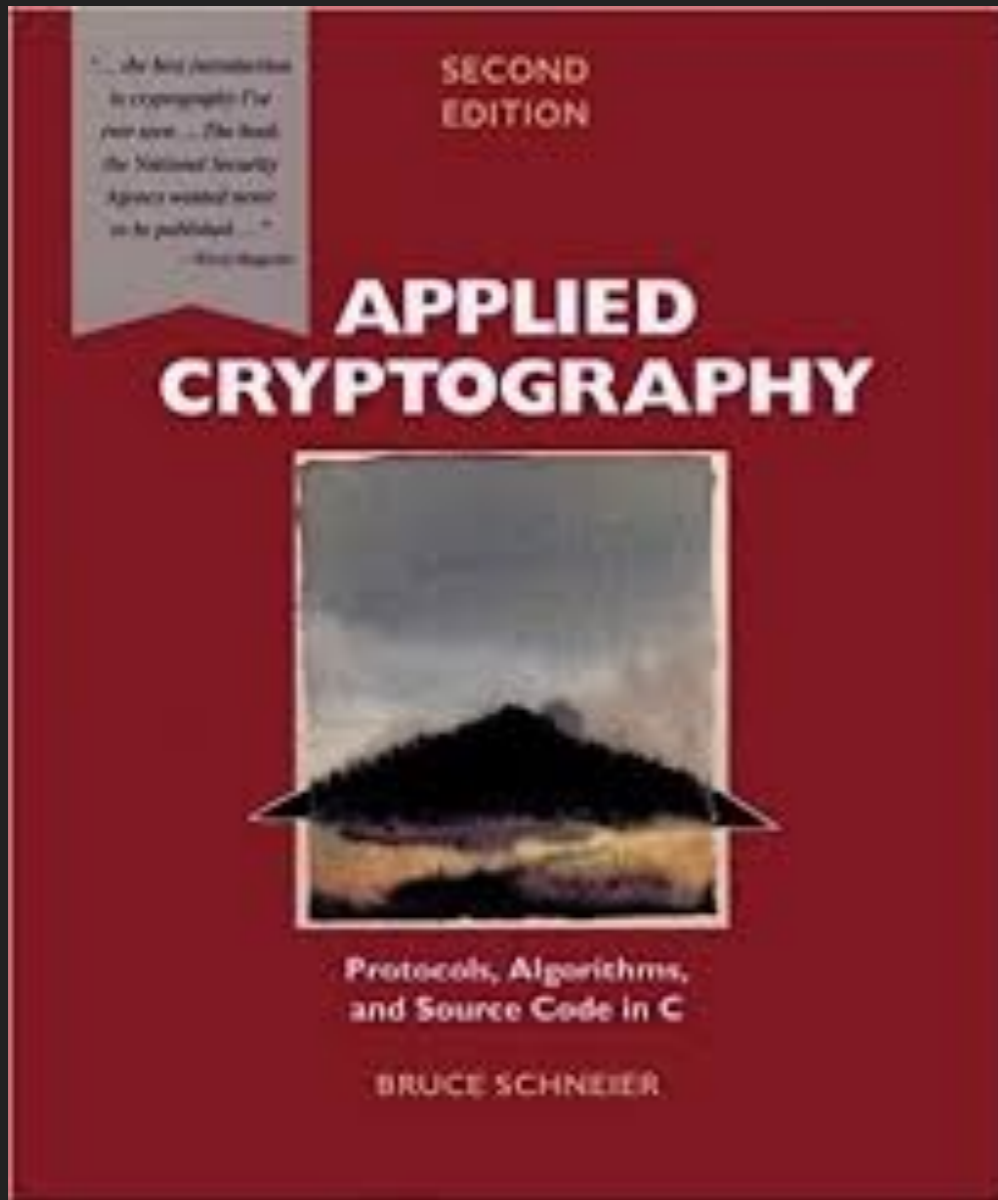


FIG. 3

EXPORT CONTROLS IN THE 1990'S

DON'T SHIP THAT FLOPPY.



PHIL ZIMMERMAN AND PGP (1990'S)

PGP





Mykrotech

MYK78T

20513

200005

CALEA

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (1994)

WE WON!

0 RLY?



FREAK: MARCH 2015

LOGJAM: MAY 2015

DROWN: MARCH 2016

NSA'S BULLRUN - SNOWDEN REVELATIONS, 2013

- ▶ EFF and others won in the courts, US Congress, and public opinion
- ▶ BULLRUN - NSA's effort to bypass democratic mechanisms and sabotage our security anyway (in secret.)
- ▶ Hidden vulnerabilities in NIST standard
- ▶ Weakening of global cryptography market to ensure people have access only to compromised methods
- ▶ Many details still unknown

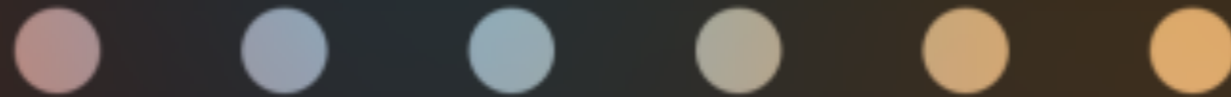
**IN THE DIGITAL AGE, ACCESS TO
AND USE OF ENCRYPTION IS AN
ENABLER OF THE RIGHT TO PRIVACY.**

Amnesty International

Sun Jul 27 19:28:11 CDT 2014



Try Again



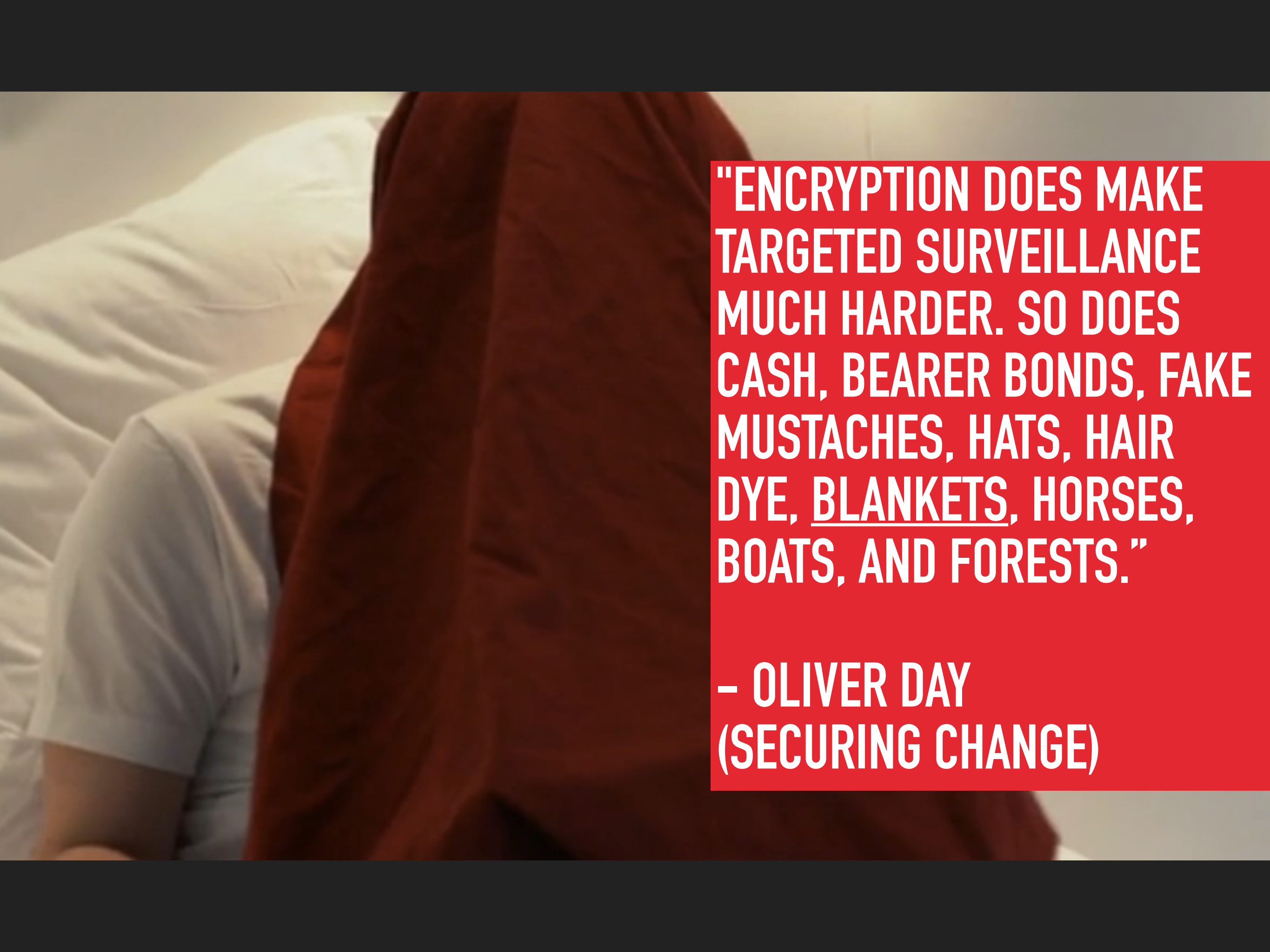


PARIS ATTACKS - NOVEMBER 2015

- ▶ Paris attacks / Telegram found on phones
- ▶ ISIL's media org, the Al-Hayat Media Group, launched a website on the dark web, recommending Telegram.
- ▶ Such activities could be used as pretext to monitor citizens and could be used to suppress dissidents.
- ▶ We cannot make messaging technology secure for everyone except for criminals / terrorists.

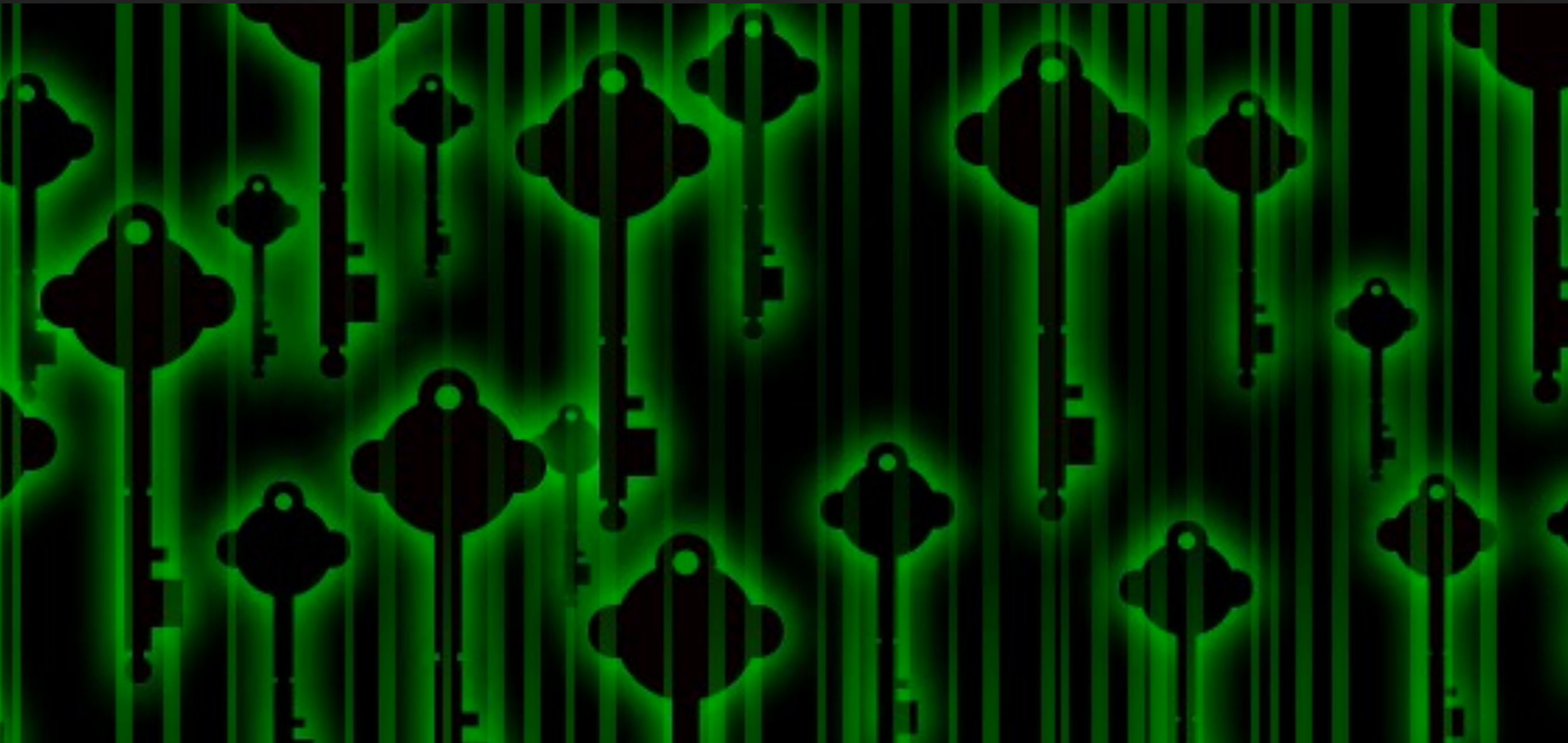


JAMES COMEY, DIRECTOR, FBI

A photograph of a person lying in bed, partially covered by a red blanket. The person is wearing a light blue shirt. The background is a plain, light-colored wall.

"ENCRYPTION DOES MAKE TARGETED SURVEILLANCE MUCH HARDER. SO DOES CASH, BEARER BONDS, FAKE MUSTACHES, HATS, HAIR DYE, BLANKETS, HORSES, BOATS, AND FORESTS."

**– OLIVER DAY
(SECURING CHANGE)**



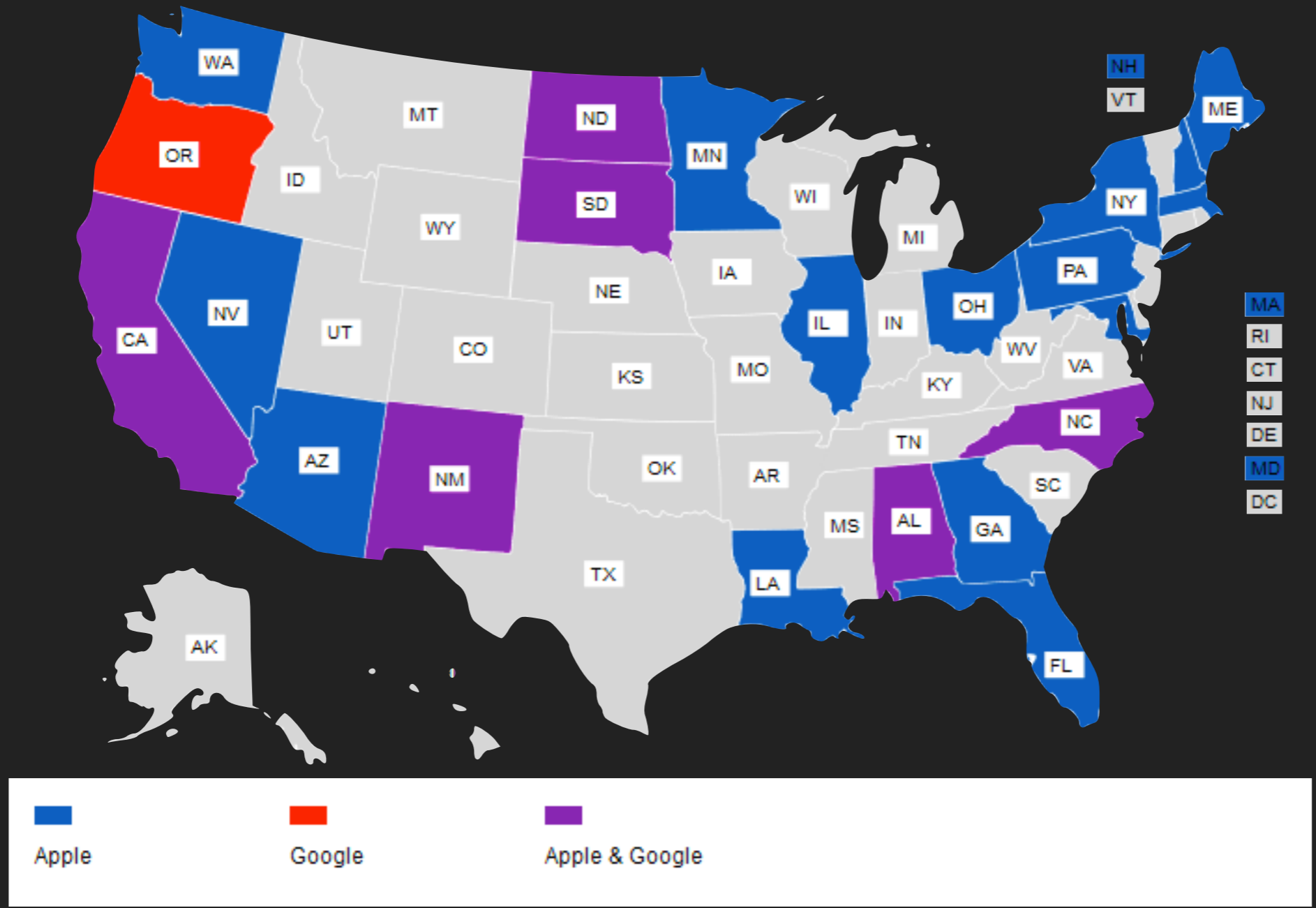
DARK

DON'T PANIC.

*Making Progress on the
“Going Dark” Debate*

**NOT JUST ONE
PHONE.**

63 ONGOING PHONE-UNLOCKING CASES IN US, 175 PHONES IN NYC



  f(t)dt Retweeted



Adam Khan @Khanoisseur

3d

FBI: Give us the keys, they'll be safe with us

Apple: No they won't

FBI: Just do it what could go wrong

Apple: 📌

FBI quietly admits that a group called "APT6" spends years inside US government networks conducting espionage:



FBI Quietly Admits to Multi-Year APT Attack, Sensitive Data Stolen



 2,203  1,373

4/14/2016: BLACKBERRY GLOBAL ENCRYPTION KEY

In fact, BlackBerry has recently signalled a willingness to deal with law enforcement on encryption, with company CEO John Chen writing last year that "we reject the notion that tech companies should refuse reasonable, lawful access requests."

"That's the reality of it, that's what we don't want the general public to know."

Through the course of the trial, the defense managed to get the Crown to admit that this wasn't just a key. It was the key. This was BlackBerry's global encryption key.

**ARE CRIMINALS
THAT SMART?**

HIDING YOURSELF ISN'T THAT EASY.

- ▶ Disable default device backups to the cloud.
- ▶ Disable default device key backups to the cloud.
- ▶ Disable default device biometric decryption (touchID).
- ▶ Avoid sending incriminating evidence by any non-encrypted means.
- ▶ Disable default cloud storage for each app.
- ▶ Don't call or text anyone (leaving behind **metadata**)






vocativ

KAITLYN KELLY / SOURCE: ACCESS NOW AND HUMAN RIGHTS WATCH

Where Can You Encrypt?

At least 6 countries in Europe and Asia have already addressed WhatsApp-style encryption

-  Laws against it already
-  Proposed legislation would penalize it
-  Government formally supports it



Source: vocativ

<http://www.vocativ.com/307667/encryption-law-europe-asia/>

MASS SURVEILLANCE, A GROWING TREND



Mass
Surveillance



Privacy

MASS SURVEILLANCE BY COUNTRY

▶ Worst

- ▶ China
- ▶ Malaysia
- ▶ Russia

▶ Slightly Better

- ▶ Singapore
- ▶ UK

▶ Meh.

- ▶ Taiwan
- ▶ Thailand
- ▶ United States.

▶ Best

- ▶ Greece, which was judged to have 'adequate safeguards against abuse'

(TS//SI//REL) Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?

(TS//SI//REL) Twenty years ago, the fact that communications were encrypted meant they were very likely to contain foreign intelligence, because only governments or other important targets had the resources to purchase or develop and implement encrypted communications. Today, anyone who uses the Internet can access web pages via the strong commercial encryption provided by HTTPS, and companies of all sizes can implement virtual private networks (VPN) to permit their employees to access sensitive or proprietary company data securely via an Internet connection from anywhere in the world. SID refers to this widespread encryption, which poses great challenges to SIGINT, as "ubiquitous encryption."

ENCRYPT



ALL THE THINGS!

WHERE ARE WE GOING?

- ▶ Expect companies to introduce additional encryption in products. Apple is well on their way with secure enclaves in their hardware.
- ▶ Expect governments to attempt to introduce legislation banning strong encryption and promoting impossible backdoors
- ▶ Oh wait, they already have...

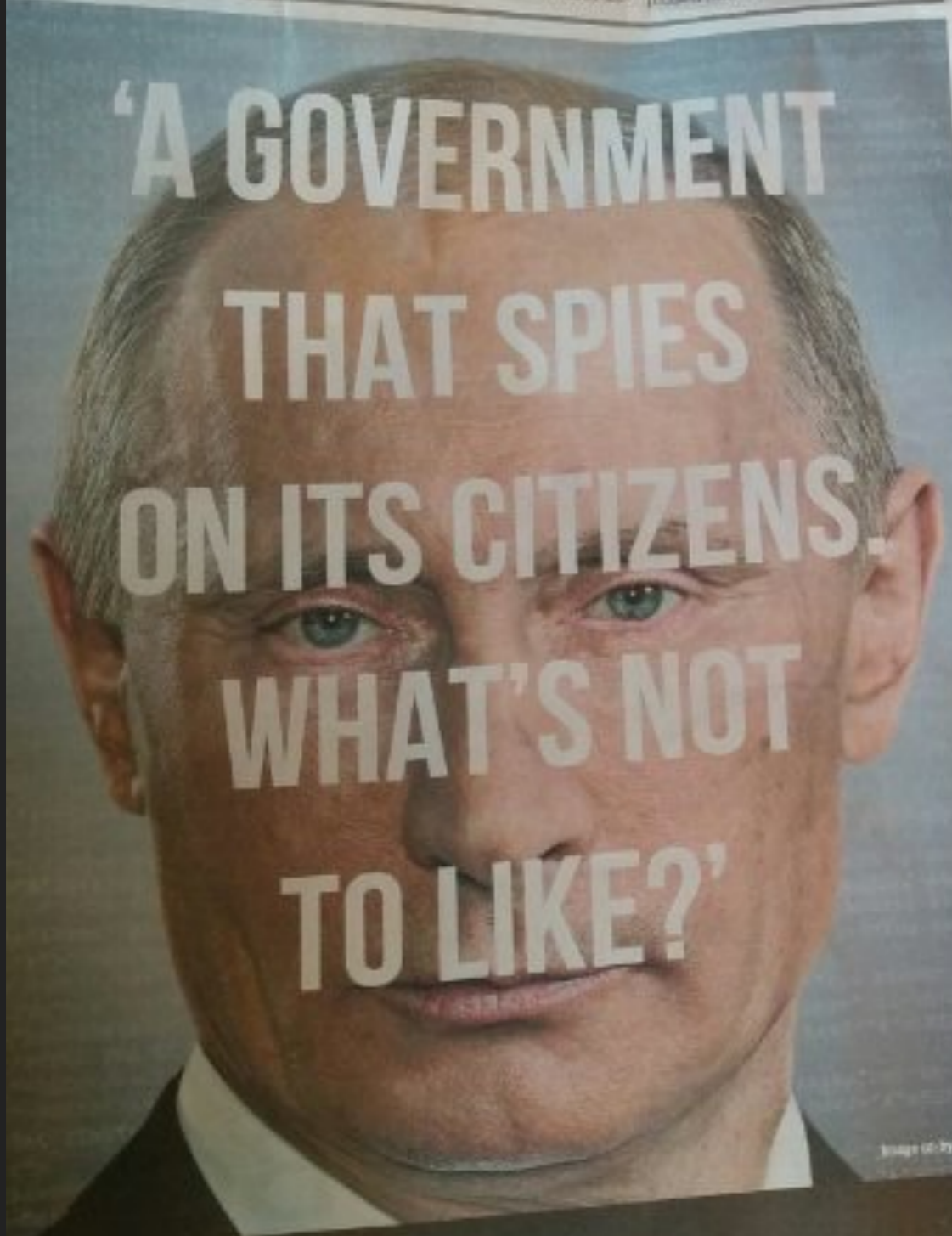
...around
FBPS, one-
h of the UK
age. One
dent, who
not wish to
samed, said:

spokesman said:
"We will assess
the situation
once the public
boundary has
been clearly
defined."

...do not want to be
connected". This means that one mil-
lion homes will have to request the
broadband connection themselves, and
in some cases pay extra to cover the
cost of connecting.
The news came as the Labour Party
lacked the Telegraph campaign for
Trickett, the shadow communities sec-

...were awarded
a night club in B
place 12 years
been consi-

...an album that ha
possession of the same fa
years was sold to a Canad
auction last November, the
placed an export bar on it to al
buyer time to raise money.
The gallery announced ye



**'A GOVERNMENT
THAT SPIES
ON ITS CITIZENS.
WHAT'S NOT
TO LIKE?'**

Image by [unreadable]



**'WELL DONE,
BRITAIN! NO ONE
MONITORS THEIR
PEOPLE QUITE
LIKE YOU.'**

The Investigatory Powers Bill, going through the UK Parliament right now, will make us a world leader in surveillance and the spy of people like China's President Xi Jinping. By allowing the bulk collection and analysis of everyone's phone and internet history this Bill will automatically put us all under surveillance, without any suspicion of wrongdoing. If, unlike Xi Jinping, you feel that mass surveillance is a step too far then take action before it's too late at dontspyonus.org.uk #DontSpyOnUs #IPBill

DON'T SPY ON US 

President Putin is a big fan of Britain's surveillance laws and Russian authorities regularly use them to justify their own snooping. So we think he's going to love the new Investigatory Powers Bill going through the UK Parliament right now. By allowing the bulk collection of everyone's phone and internet history, it will place the whole population under surveillance. If, unlike Mr Putin, you feel that mass surveillance is a step too far then take action before it's too late at dontspyonus.org.uk #DontSpyOnUs #IPBill

DON'T SPY ON US 

UK CALLS FOR OUTLAWING NON-BACKDOORED CRYPTO (2015)

- ▶ Prime minister David Cameron, Jan. 2015 calls for ban on end-to-end encryption that the government cannot read.
- ▶ If you can't say something to a friend or family member without the fear the government, your neighbor or your boss will overhear, your free expression is deeply curtailed.
- ▶ There is no such thing as "good guy encryption" and "bad guy encryption".

DRAFT COMMUNICATIONS BILL (UK)

- ▶ "Snooper's Charter"
- ▶ "maintain records of each user's internet browsing activity (including social media), email correspondence, voice calls, internet gaming, and mobile phone messaging services and store the records for 12 months. Retention of email and telephone contact data for this time is already required by the Data Retention Regulations 2014."
- ▶ The anticipated cost is £1.8 billion.
- ▶ UK Home Secretary Theresa May

BURR-FEINSTEIN BILL (USA, APRIL 2016)

- ▶ Ridiculous.
- ▶ Privacy advocates who expected the worst weren't disappointed.
- ▶ Make all of our online data "intelligible" when presented with a court order.
- ▶ The bill defines intelligible as "decrypted, deciphered, decoded, demodulated, or deobfuscated"
- ▶ As currently written, the draft likely even outlaws forward secrecy. (source: EFF - More on this in a second.)

Politics

Dutch government backs strong encryption, condemns backdoors

By Patrick Howell O'Neill

Jan 4, 2016, 9:55am CT | Last updated Jan 4, 2016, 3:27pm CT

The Netherlands government issued a strong [statement](#) on Monday against weakening [encryption](#) for the purposes of law enforcement and intelligence agencies.

Why a staggering number of Americans have stopped using the Internet the way they used to

By **Andrea Peterson** May 13



(iStock)

Nearly one in two Internet users say privacy and security concerns have now stopped them from doing basic things online — such as posting to social networks, expressing opinions in forums or even buying things from websites, according to a new government survey released Friday.

Most Read

1 China killed thousands of Maine jobs. Now it's eating up the state's lobsters.



2 Even for the fast-melting Arctic, 2016 is in 'uncharted territory'



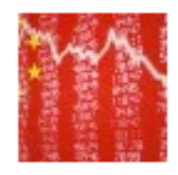
3 In some towns, the strip malls can't die fast enough



4 Why smart kids shouldn't use laptops in class



5 China's debt bubble is getting only more dangerous



Market Watch

**WHAT CAN YOU
DO?**

IN CHARGE OF HTTP-BASED SERVERS AND SERVICES? (OR VPN?)

- ▶ Implement proper, always-on HTTPS - you have no excuse!
- ▶ Enable HPKP (pinning for TLS certificates)
- ▶ Enable HSTS (always talk to me in HTTPS)
- ▶ Enable PFS (Perfect forward secrecy)
- ▶ Verify your implementation (<https://www.ssllabs.com>)
- ▶ If possible, ask to be added to the HSTS preload list (chrome)

WHAT CAN YOU DO?

THIS ISN'T HARD, IT'S NEARLY FREE NOW.

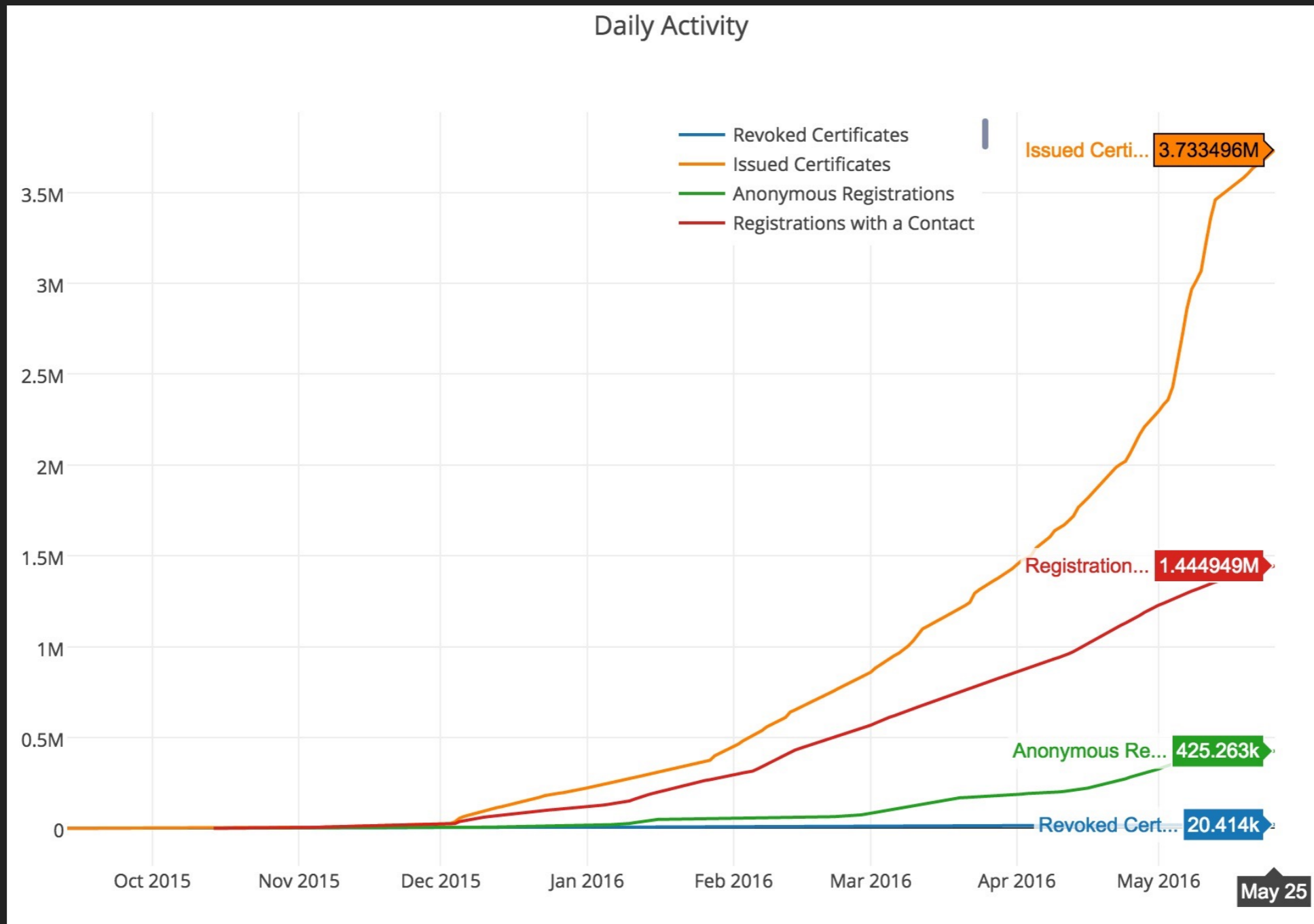
LET'S ENCRYPT

<https://letsencrypt.org/>

MOZILLA RECOMMENDED CIPHER SUITES

<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

MAKING GOOD PROGRESS - LET'S ENCRYPT



ARE YOU A DEVELOPER?

- ▶ Encrypt data at Rest and in Transit, even inside your company's network.
 - ▶ Please don't reinvent the "secure messaging" wheel.
 - ▶ It's been done too many times.
 - ▶ You're probably (not) a cryptographer.
 - ▶ Signal is doing it better than you anyway.

END-USER

- ▶ Know your vulnerabilities and threat model
- ▶ Promote end-to-end, encryption-by-default on projects that you work on
- ▶ Encrypt your phone, text messages (Signal), and hard disk
- ▶ Use strong passwords with a password manager and promote the use of 2-factor in your organization
- ▶ Use Tor.
- ▶ Enable and install HTTPS Everywhere, Adblockers, uBlock, etc.

POLITICALLY...

- ▶ Demand that your representatives in government block anti-encryption bills
- ▶ Help the **EFF**, **ACLU**, and other privacy-promoting organizations with your donations and time.
- ▶ We can fight with technology, but fighting them with legislation and precedent cases will probably be more effective in the long-run.
- ▶ Let's all work together to make the Internet more secure.

THANK YOU!

JOHN ADAMS — @NETIK