WHAT IF PETRAEUS WAS A HACKER?

Email privacy for the rest of us

https://en.wikipedia.org/wiki/David_Petraeus

DERBYCON

Phil Cryer / @fak3r

v2.01

Louisville, KY
September 2013


[redacted]

Phil Cryer

Phil Cryer

Phil Cryer

OPEN SOURCE TECHNOLOGIST

better known online as...

@FAK3R


Phil Cryer
OPEN SOURCE TECHNOLOGIST
INFOSEC RESEARCHER+SPEAKER
better known online as...
@FAK3R


Phil Cryer
OPEN SOURCE TECHNOLOGIST
INFOSEC RESEARCHER+SPEAKER
PRIVACY ADVOCATE
better known online as...
@FAK3R

THINGS TO THINK ABOUT

h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

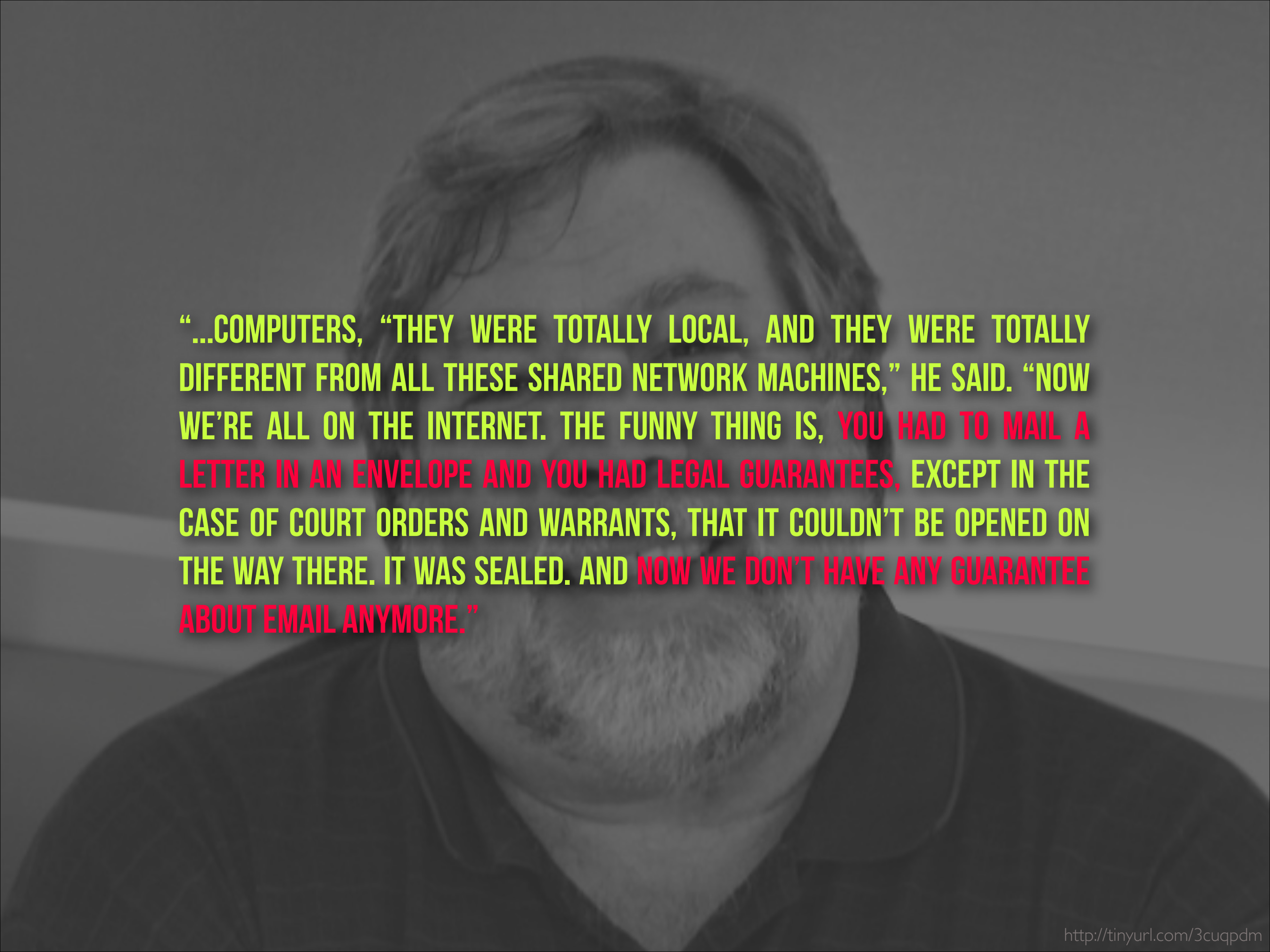
3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

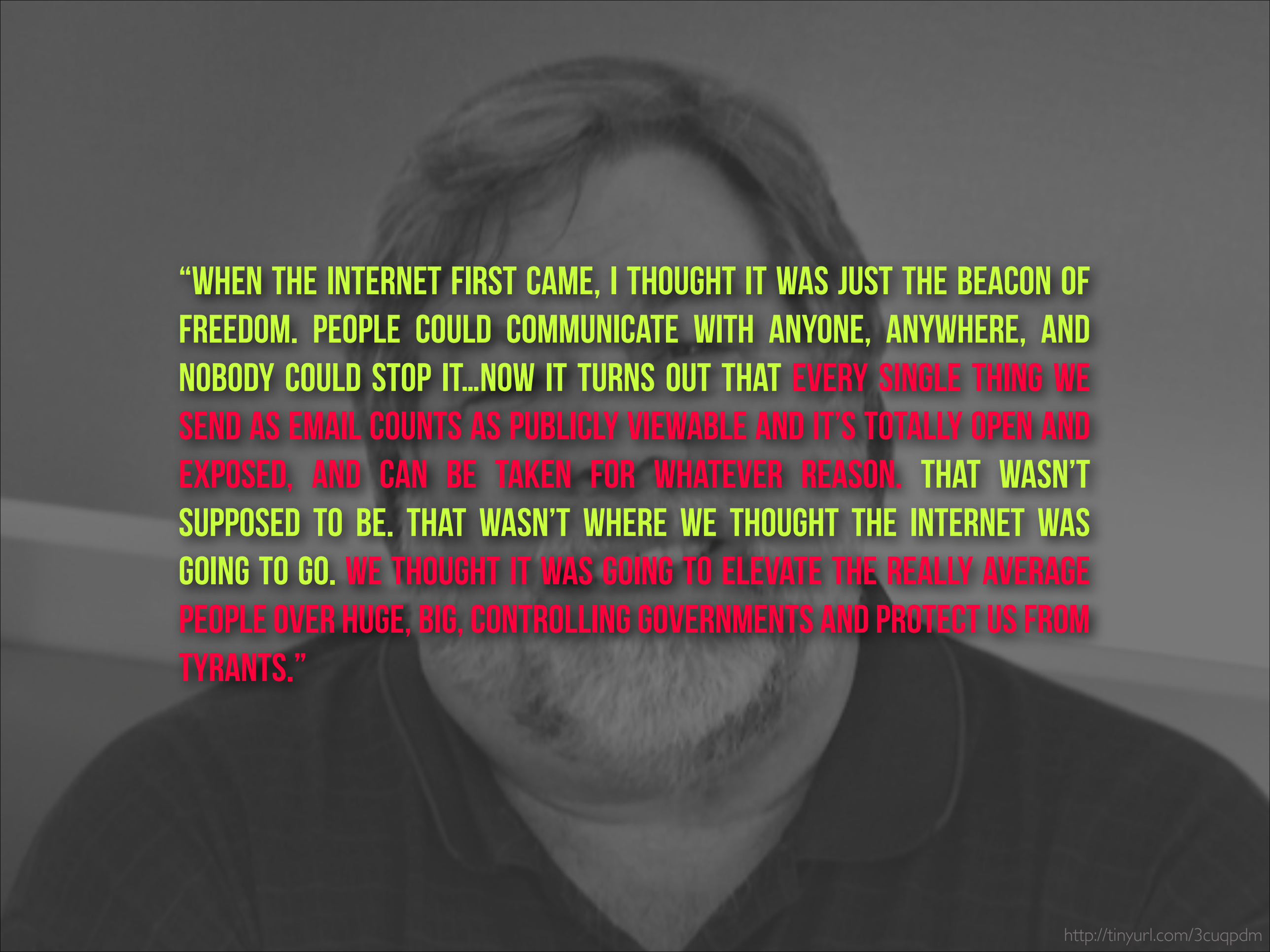
IS THERE PRIVACY IN EMAIL

http://tinyurl.com/3cuqpdm



"...COMPUTERS, "THEY WERE TOTALLY LOCAL, AND THEY WERE TOTALLY DIFFERENT FROM ALL THESE SHARED NETWORK MACHINES," HE SAID. "NOW WE'RE ALL ON THE INTERNET. THE FUNNY THING IS, YOU HAD TO MAIL A LETTER IN AN ENVELOPE AND YOU HAD LEGAL GUARANTEES, EXCEPT IN THE CASE OF COURT ORDERS AND WARRANTS, THAT IT COULDN'T BE OPENED ON THE WAY THERE. IT WAS SEALED. AND NOW WE DON'T HAVE ANY GUARANTEE ABOUT EMAIL ANYMORE."

http://tinyurl.com/3cuqpdm



"WHEN THE INTERNET FIRST CAME, I THOUGHT IT WAS JUST THE BEACON OF FREEDOM. PEOPLE COULD COMMUNICATE WITH ANYONE, ANYWHERE, AND NOBODY COULD STOP IT...NOW IT TURNS OUT THAT EVERY SINGLE THING WE SEND AS EMAIL COUNTS AS PUBLICLY VIEWABLE AND IT'S TOTALLY OPEN AND EXPOSED, AND CAN BE TAKEN FOR WHATEVER REASON. THAT WASN'T SUPPOSED TO BE. THAT WASN'T WHERE WE THOUGHT THE INTERNET WAS GOING TO GO. WE THOUGHT IT WAS GOING TO ELEVATE THE REALLY AVERAGE PEOPLE OVER HUGE, BIG, CONTROLLING GOVERNMENTS AND PROTECT US FROM TYRANTS."

http://tinyurl.com/3cuqpdm

HE SUGGESTED THE TWO TOP TECHNOLOGY COMPANIES, MICROSOFT AND APPLE, MISSED AN OPPORTUNITY BY NOT INCORPORATING PGP (FOR "PRETTY GOOD PRIVACY) ENCRYPTION SOFTWARE INTO THEIR PRODUCTS. "IF TWO COMPANIES, MICROSOFT AND APPLE, AND BUILT IN PGP ENCRYPTION," WOZNIAK SAID, "EVERY EMAIL WOULD HAVE BEEN ENCRYPTED AND UNCRACKABLE."

http://tinyurl.com/3cuqpdm

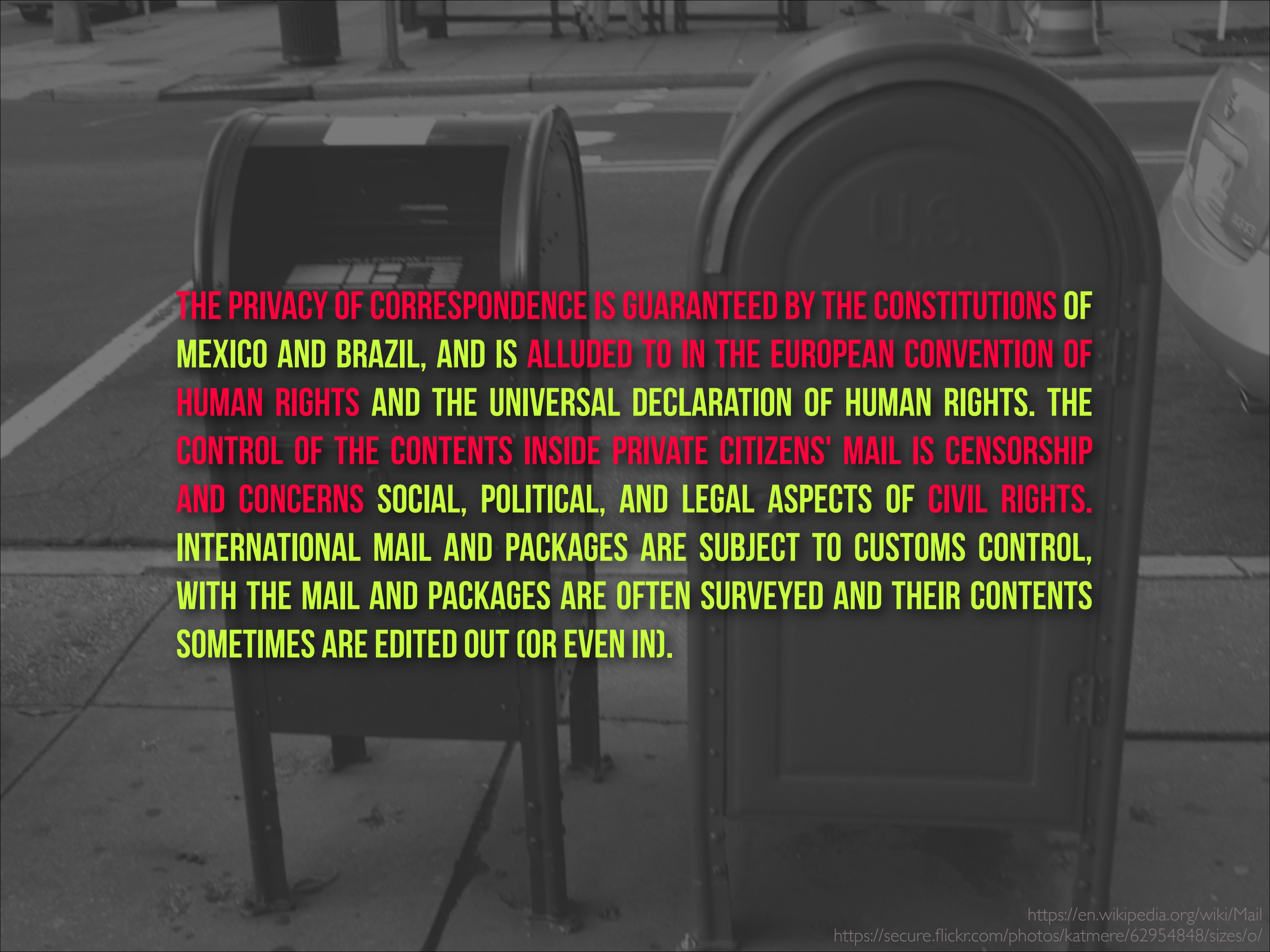
http://tinyurl.com/3cuqpdm

SO WITH ABOUT MAIL

https://secure.flickr.com/photos/katmere/62954848/sizes/o/

DOCUMENTS SHOULD GENERALLY NOT BE READ BY ANYONE OTHER THAN THE ADDRESSEE; FOR INSTANCE, IN THE UNITED STATES OF AMERICA IT IS A VIOLATION OF FEDERAL LAW FOR ANYONE OTHER THAN THE ADDRESSEE [...] TO OPEN MAIL. THERE ARE EXCEPTIONS THOUGH: EXECUTIVES OFTEN DELEGATE TO SECRETARIES OR ASSISTANTS THE TASK OF DEALING WITH THEIR MAIL; AND POSTCARDS DO NOT REQUIRE OPENING AND CAN BE READ BY ANYBODY. FOR MAIL CONTAINED WITHIN AN ENVELOPE, THERE ARE LEGAL PROVISIONS IN SOME JURISDICTIONS ALLOWING THE RECORDING OF IDENTITIES OF SENDER AND RECIPIENT.

https://en.wikipedia.org/wiki/Mail
https://secure.flickr.com/photos/katmere/62954848/sizes/o/



THE PRIVACY OF CORRESPONDENCE IS GUARANTEED BY THE CONSTITUTIONS OF MEXICO AND BRAZIL, AND IS ALLUDED TO IN THE EUROPEAN CONVENTION OF HUMAN RIGHTS AND THE UNIVERSAL DECLARATION OF HUMAN RIGHTS. THE CONTROL OF THE CONTENTS INSIDE PRIVATE CITIZENS' MAIL IS CENSORSHIP AND CONCERNS SOCIAL, POLITICAL, AND LEGAL ASPECTS OF CIVIL RIGHTS. INTERNATIONAL MAIL AND PACKAGES ARE SUBJECT TO CUSTOMS CONTROL, WITH THE MAIL AND PACKAGES ARE OFTEN SURVEYED AND THEIR CONTENTS SOMETIMES ARE EDITED OUT (OR EVEN IN).

https://en.wikipedia.org/wiki/Mail
https://secure.flickr.com/photos/katmere/62954848/sizes/o/

https://secure.flickr.com/photos/katmere/62954848/sizes/o/

WHAT ARE THE LAWS ON EMAIL

http://www.flickr.com/photos/limaoscarjuliet/225249268/sizes/o/

IN THE UNITED STATES, THERE IS NO CONSTITUTIONAL GUARANTEE ON EMAIL PRIVACY OR CORRESPONDENCE IN GENERAL. THE SECRECY OF CORRESPONDENCE IS DERIVED FROM THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION AND AN 1877 U.S. SUPREME COURT CASE.

HOWEVER, LIKE ALL RIGHTS THAT HAVE BEEN DERIVED THROUGH LITIGATION, THIS IS SUBJECT TO INTERPRETATIONS AND IS LIMITED BY THE LEGAL REQUIREMENT OF A "REASONABLE EXPECTATION OF PRIVACY" WHICH MAY BE EITHER SUBJECTIVE (THE OPINION OF THE PERSON IN QUESTION) OR OBJECTIVE (AS RECOGNIZED BY SOCIETY).

https://secure.runbox.com/why-runbox/email-privacy-offshore-email/
http://www.flickr.com/photos/limaoscarjuliet/225249268/sizes/o/

IN THE UNITED STATES [...] EMAIL IS ALSO PROTECTED BY THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) OF 1986 WHICH WAS ENACTED TO EXTEND GOVERNMENT RESTRICTIONS TO INCLUDE TRANSMISSIONS OF ELECTRONIC DATA. THE ECPA HAS BEEN CRITICIZED BECAUSE AN AGENCY DOESN'T NEED JUDICIAL REVIEW IN ORDER TO DEMAND CONSUMER DATA FROM SERVICE PROVIDERS.

FURTHERMORE, AFTER 6 MONTHS, EMAIL MESSAGES LOSE THEIR STATUS AS PROTECTED COMMUNICATION UNDER THE ECPA AND BECOME A REGULAR DATABASE RECORD. THIS MEANS THAT JUST A SUBPOENA INSTEAD OF A WARRANT IS REQUIRED FOR A GOVERNMENT AGENCY TO FORCE EMAIL PROVIDERS TO PRODUCE A COPY OF A RECORD.

https://secure.runbox.com/why-runbox/email-privacy-offshore-email/
http://www.flickr.com/photos/limaoscarjuliet/225249268/sizes/o/

EMAIL PROVIDERS [CAN] SCREEN EMAIL COMMUNICATION IN ORDER TO DISPLAY TARGETED ADVERTISEMENTS TO THE USER, OR STORE MESSAGE CONTENTS AND PERSONAL DATA IN ORDER TO EXTRACT INFORMATION THAT MAY BE SHARED WITH THIRD PARTIES FOR COMMERCIAL GAIN ("DATA MINING")

ALSO, EMAIL MESSAGES SENT OVER COMPANY COMPUTERS ARE GENERALLY CONSIDERED TO BE COMPANY PROPERTY AND ARE THEREFORE ACCESSIBLE BY THE COMPANY'S MANAGEMENT.

INTELLIGENCE AGENCIES MAY UTILIZE SURVEILLANCE SOFTWARE TO MONITOR EMAIL MESSAGES TO COMBAT ESPIONAGE, FACILITATE POLITICAL EAVESDROPPING, OR CARRY OUT OTHER TYPES OF SCREENING IN THE PERCEIVED INTEREST OF NATIONAL SECURITY.

https://secure.runbox.com/why-runbox/email-privacy-offshore-email/
http://www.flickr.com/photos/limaoscarjuliet/225249268/sizes/o/

http://www.flickr.com/photos/limaoscarjuliet/225249268/sizes/o/

THE PETRAEUS INCIDENT

Tampa Bay Times

Try a big slic

bay.com

In the know

PORT OFFICIALS CERTAIN ON THE CEO THEY WANT

A special kid has her special day

This ought to be David Price's time

Borders don't confine Syria war

Summit tackles distracted driving

Still no arrests in Lifestyle attacks

Socialite's emails snare 2nd general

Key players and their connections

Associated Press

Gen. David Petraeus was running the war in Afghanistan before becoming director of the CIA in September 2011.

David Petraeus — Family friends with ...

Retired four-star Army general, 60, who became CIA director in September 2011 after an accomplished military career that included stints as commander of U.S. and international troops in Iraq and Afghanistan. He resigned from his post at the CIA last Friday after admitting to having "extremely poor judgment by engaging in an extramarital affair." Married to Holly for 36 years, with two grown children.

... Had a "close" relationship with ...

Paula Broadwell

Author of three biographies, [illegible] University of Central

Associated Press

Jill Kelley leaves her home Tuesday. Hear audio of police calls about trespassers at the home at tampabay.com.

5 aides put on leave in inquiry

But no charges will be filed in the drowning of the Riverview special needs student.

BY JESSICA VANDER VELDE AND MARLENE SOKOL
Times Staff Writers

RIVERVIEW — Two weeks before an 11-year-old girl with Down syndrome walked away from her physical education class and drowned in a pond at her school, her PE teacher issued a warning.

The teacher's aides tasked with caring for her and other special-needs students in the gym were inattentive, coach Garry Gawrych told an assistant principal at Rodgers Middle School.

Six aides were assigned to care for 24 special-need students, but the adults would usually just sit on the bleachers, he said.

When students walked away or hid, it was Gawrych who followed, the coach said.

"I can't keep

Jennifer Caballero, 10, drowned near her school Oct. 22.

David

https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

David

https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

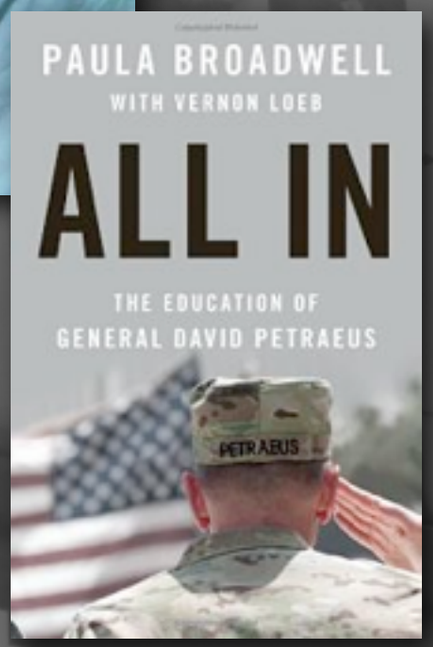
Paula

David

https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

David

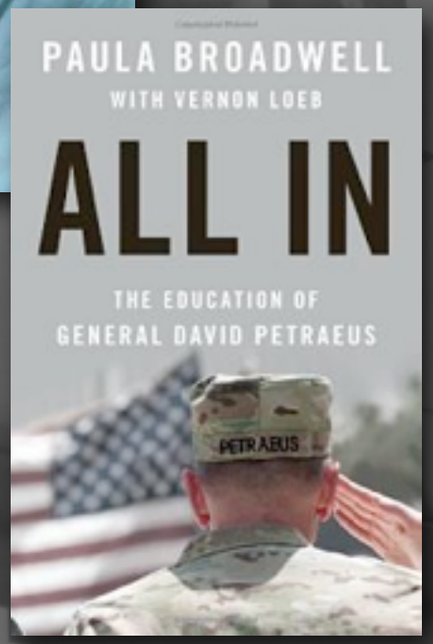
Paula



https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

Paula

David

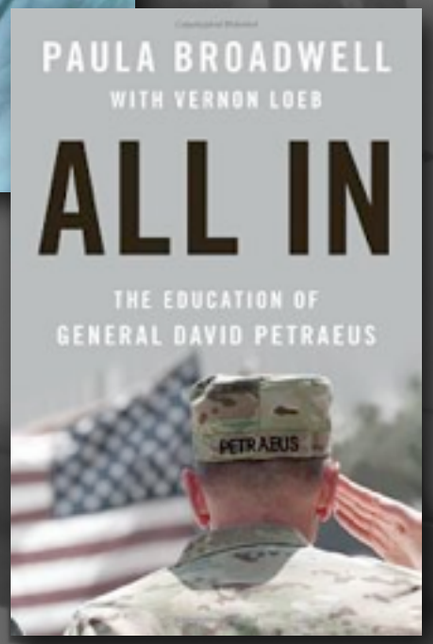


https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

Paula

David

Jill



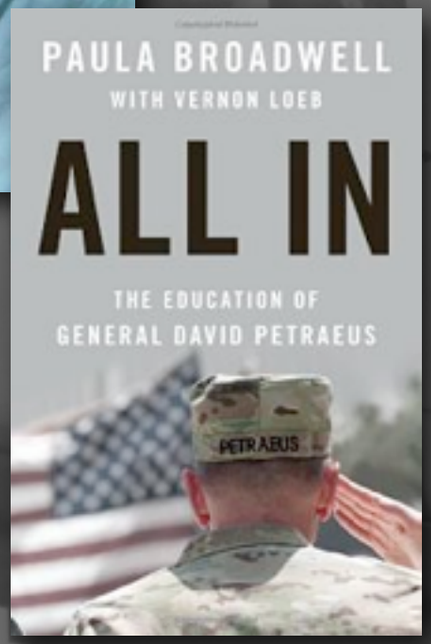
https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

Paula

David

Jill

ohai



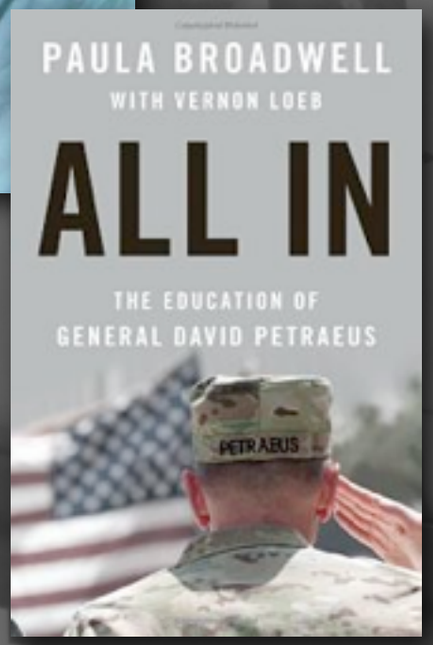
https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://militaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

David

Paula

Jill

ohai



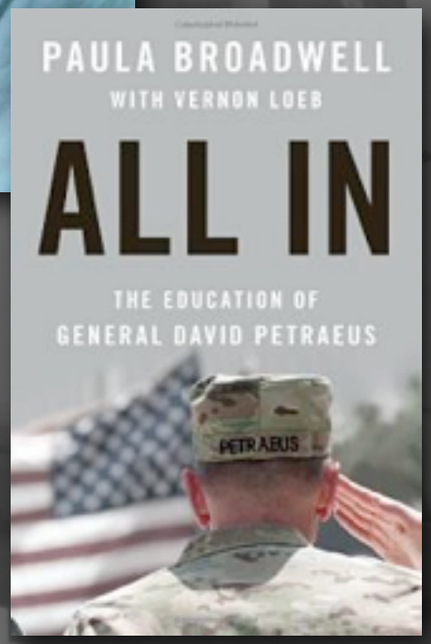
ikipedia.org/wiki/David_Petraeus
.org/wiki/File:Paula_Broadwell.jpg
t.com/2011_05_01_archive.html
https://secure. 2705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

Paula

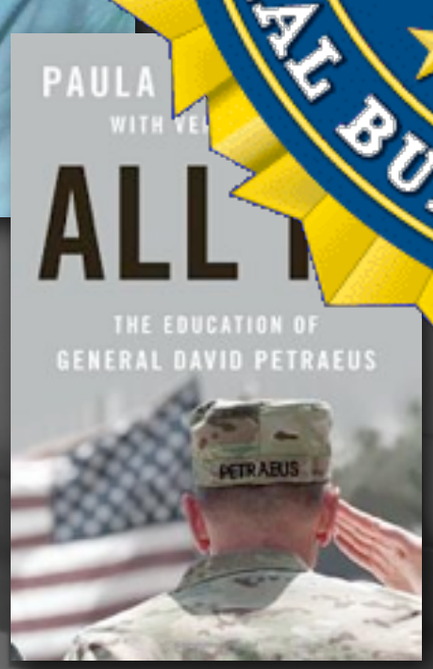
David

Jill

ohai



ikipedia.org/wiki/David_Petraeus
.org/wiki/File:Paula_Broadwell.jpg
t.com/2011_05_01_archive.html
https://secure. 2705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx



ohai

id

https://secure. 2705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

https://en.wikipedia.org/wiki/David_Petraeus
https://en.wikipedia.org/wiki/File:Paula_Broadwell.jpg
http://dmilitaryinsignia.blogspot.com/2011_05_01_archive.html
https://secure.flickr.com/photos/dno1967b/3187252705/sizes/h/in/photolist-dttNZp
http://www.theatlanticwire.com/national/2012/11/what-we-know-about-petraeus-affair/58909/
http://www.hindustantimes.com/Brunch/Brunch-Stories/Spectator-Sexism-Rules-OK/Article1-963692.aspx

http://www.globalpost.com/dispatch/news/regions/americas/united-states/121112/jill-kelley-who-she
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp

COLLATERAL

DAMAGE

http://www.globalpost.com/dispatch/news/regions/americas/united-states/121112/jill-kelley-who-she
https://secure.flickr.com/photos/dno1967b/8187252705/sizes/h/in/photolist-dttNZp

Bay Times

bay.com

5 aides put on leave in inquiry

But no charges will be filed in the drowning of the Riverview special needs student.

BY JESSICA VANDER VELDE AND MARLENE SOKOL
Times Staff Writers

RIVERVIEW — Two weeks before an 11-year-old girl with Down syndrome walked away from her physical education class and drowned in a pond at her school, her PE teacher issued a warning.

The teacher's aides tasked with caring for her and other special-needs students in the gym were inattentive, coach Garry Gasgrych told an assistant principal at Rodgers Middle School.

Six aides were assigned to care for 24 special-need students, but the adults would usually just sit on the bleachers, he said.

When students walked away or hit, it was Gasgrych who followed, the coach said.

"I can't keep

Jennifer Caballero, 10, drowned near her school Oct. 22.

Socialite's emails snare 2nd general

Key players and their connections

Gen. David Petraeus was running the war in Afghanistan before becoming director of the CIA in September 2011.

David Petraeus

Paula Broadwell

Jill Kelley leaves her home Tuesday. Hear audio of police calls about trespassers at the home at tampabay.com.

A special kid has her special day

This ought to be David Price's time

Borders don't confine Syria war

Summit tackles distracted driving

Still no arrests in Aurora attacks

PORT OFFICIALS CERTAIN ON THE CEO THEY WANT

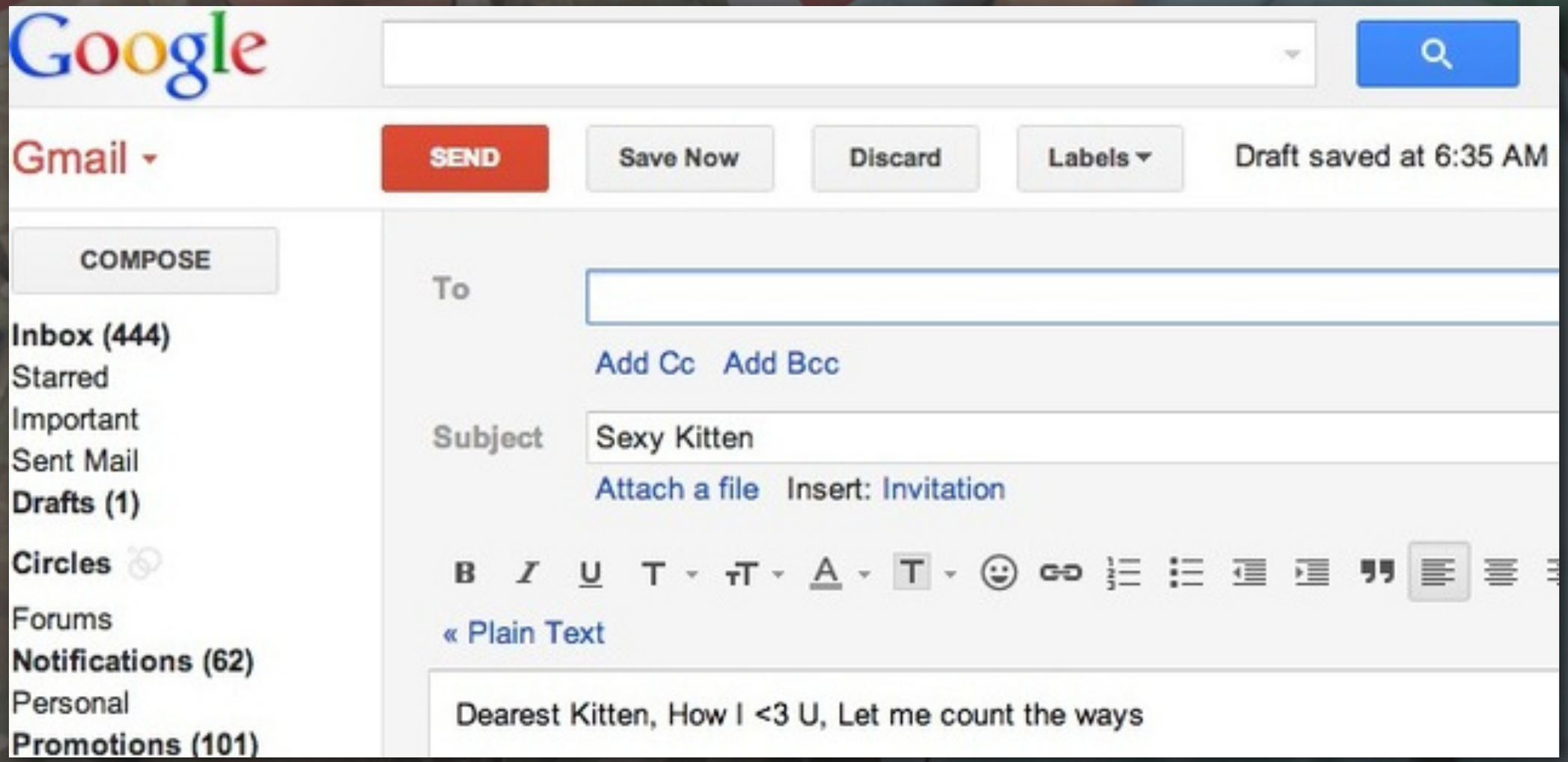
Try a big slic

HOW PETRAEUS WAS CAUGHT

https://en.wikipedia.org/wiki/David_Petraeus

RATHER THAN TRANSMITTING E-MAILS TO THE OTHER'S INBOX, THEY COMPOSED AT LEAST SOME MESSAGES AND LEFT THEM IN A DRAFT FOLDER OR IN AN ELECTRONIC "DROP BOX," THE AP REPORTED. THEN THE OTHER PERSON COULD LOG ONTO THE SAME ACCOUNT AND READ THE DRAFT E-MAILS, AVOIDING THE CREATION OF AN E-MAIL TRAIL THAT MIGHT BE EASIER TO TRACE.

http://www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1703111/
https://en.wikipedia.org/wiki/David_Petraeus



http://www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1700111/

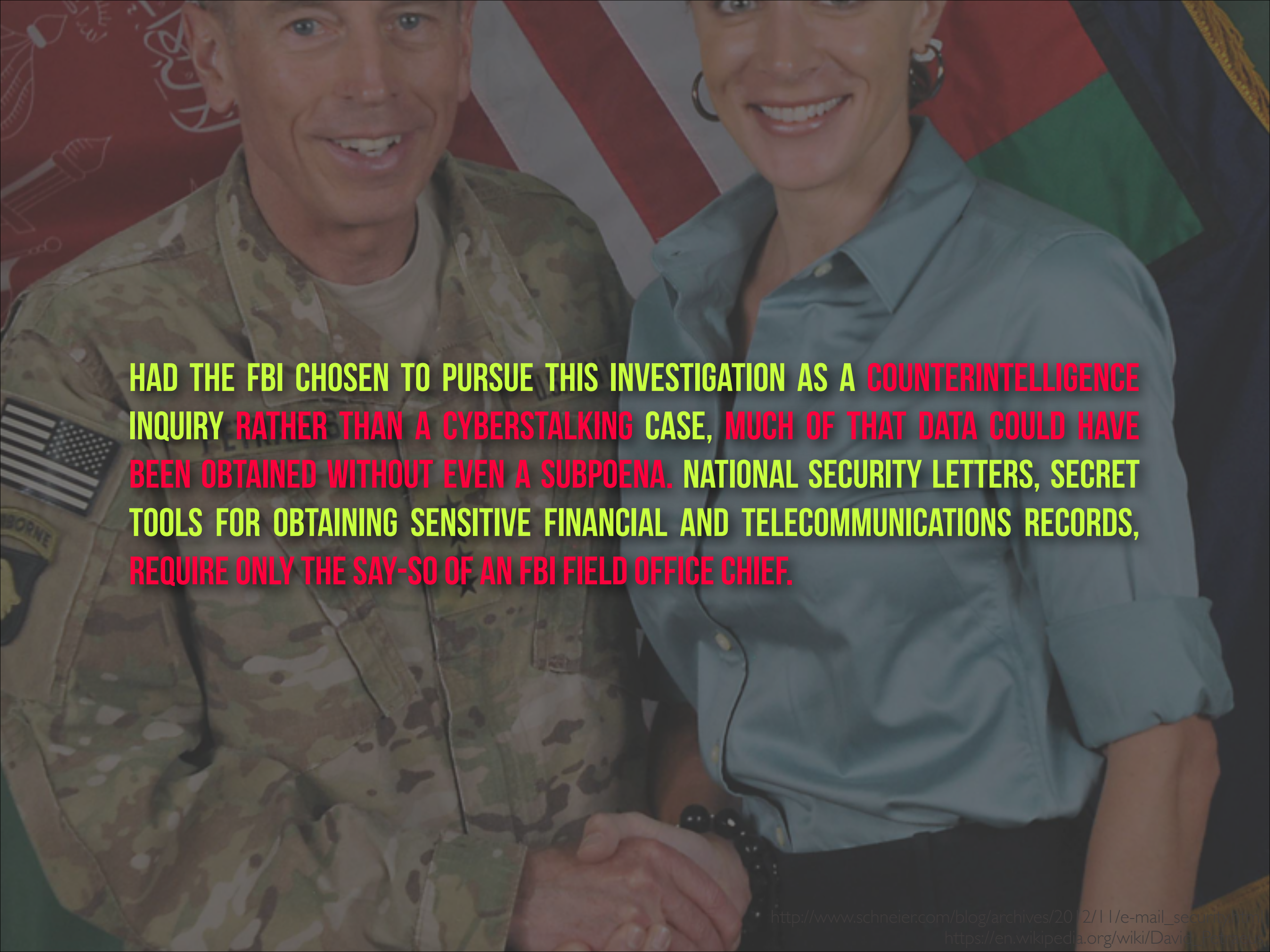
https://en.wikipedia.org/wiki/David_Petraeus

IN THE PETRAEUS CASE [...] FBI OBTAINED SUBPOENAS FOR INTERNET PROTOCOL LOGS, ALLOWING THEM TO CONNECT THE SENDER'S ANONYMOUS GOOGLE MAIL ACCOUNT TO OTHERS ACCESSED FROM THE SAME COMPUTERS, ACCOUNTS THAT BELONGED TO PETRAEUS BIOGRAPHER PAULA BROADWELL.

FROM THERE THEY SUBPOENAED GUEST RECORDS FROM HOTELS, TRACKING THE WIFI NETWORKS, AND CONFIRM THAT THEY MATCHED BROADWELL'S TRAVEL HISTORY. NONE OF THIS REQUIRED JUDICIAL APPROVAL LET ALONE A FOURTH AMENDMENT SEARCH WARRANT BASED ON PROBABLE CAUSE.

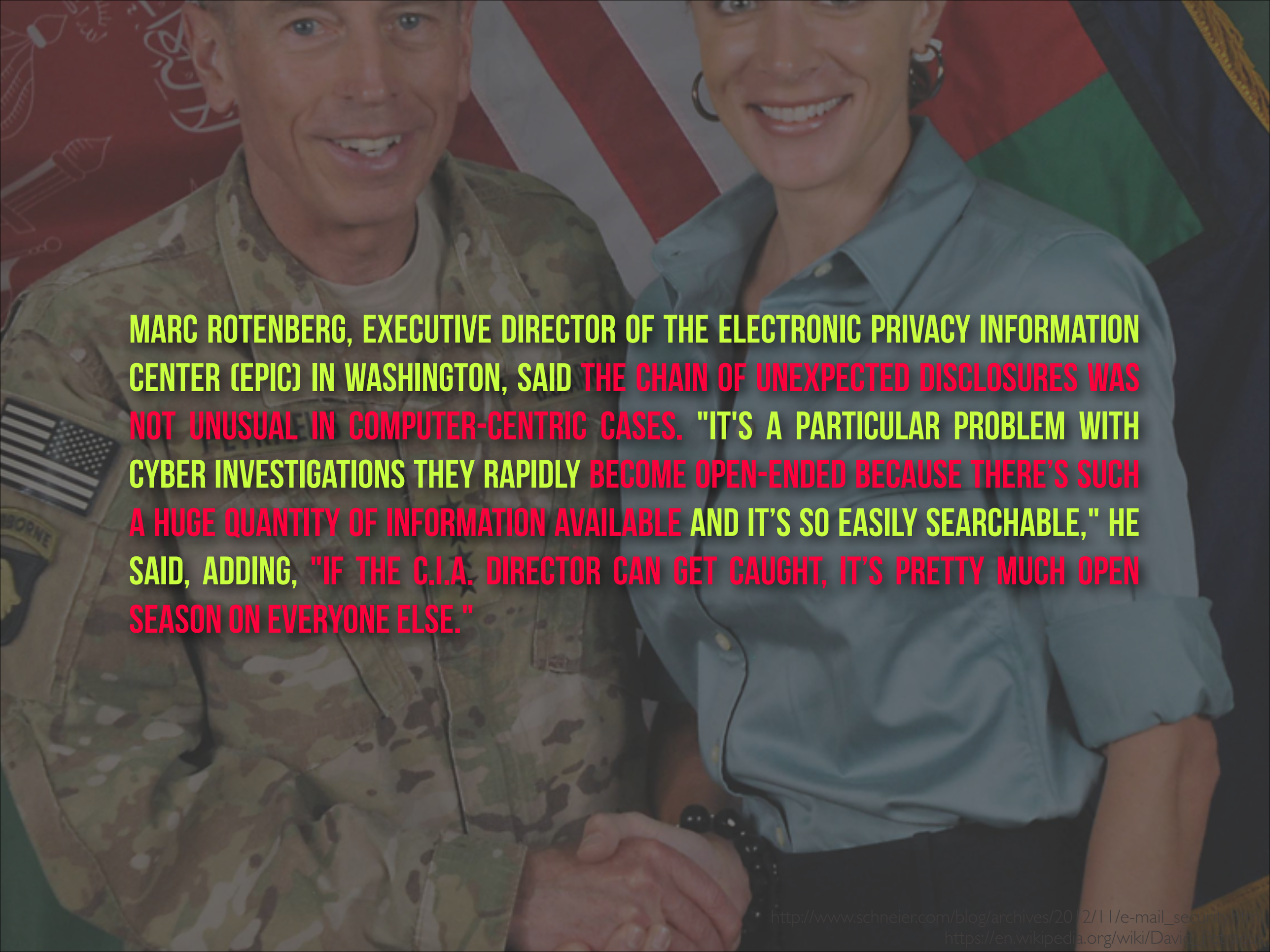
THERE IS NO INDEPENDENT REVIEW, NO CHECK AGAINST ABUSE, AND FURTHER, THE TARGET OF THE SUBPOENA WILL OFTEN NEVER LEARN THAT THE GOVERNMENT OBTAINED DATA (UNLESS CHARGES ARE FILED, OR, AS IN THIS PARTICULAR CASE, GOVERNMENT OFFICIALS EAGERLY LEAK DETAILS OF THE INVESTIGATION TO THE PRESS).

http://www.schneier.com/blog/archives/2012/11/e-mail_security.html
https://en.wikipedia.org/wiki/David_Petraeus



HAD THE FBI CHOSEN TO PURSUE THIS INVESTIGATION AS A COUNTERINTELLIGENCE INQUIRY RATHER THAN A CYBERSTALKING CASE, MUCH OF THAT DATA COULD HAVE BEEN OBTAINED WITHOUT EVEN A SUBPOENA. NATIONAL SECURITY LETTERS, SECRET TOOLS FOR OBTAINING SENSITIVE FINANCIAL AND TELECOMMUNICATIONS RECORDS, REQUIRE ONLY THE SAY-SO OF AN FBI FIELD OFFICE CHIEF.

http://www.schneier.com/blog/archives/2012/11/e-mail_security_1.html
https://en.wikipedia.org/wiki/David_Petraeus



MARC ROTENBERG, EXECUTIVE DIRECTOR OF THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN WASHINGTON, SAID THE CHAIN OF UNEXPECTED DISCLOSURES WAS NOT UNUSUAL IN COMPUTER-CENTRIC CASES. "IT'S A PARTICULAR PROBLEM WITH CYBER INVESTIGATIONS THEY RAPIDLY BECOME OPEN-ENDED BECAUSE THERE'S SUCH A HUGE QUANTITY OF INFORMATION AVAILABLE AND IT'S SO EASILY SEARCHABLE," HE SAID, ADDING, "IF THE C.I.A. DIRECTOR CAN GET CAUGHT, IT'S PRETTY MUCH OPEN SEASON ON EVERYONE ELSE."

http://www.schneier.com/blog/archives/2012/11/e-mail_security.html
https://en.wikipedia.org/wiki/David_Petraeus

https://en.wikipedia.org/wiki/David_Petraeus

WHISTLEBLOWER EDWARD SNOWDEN

https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

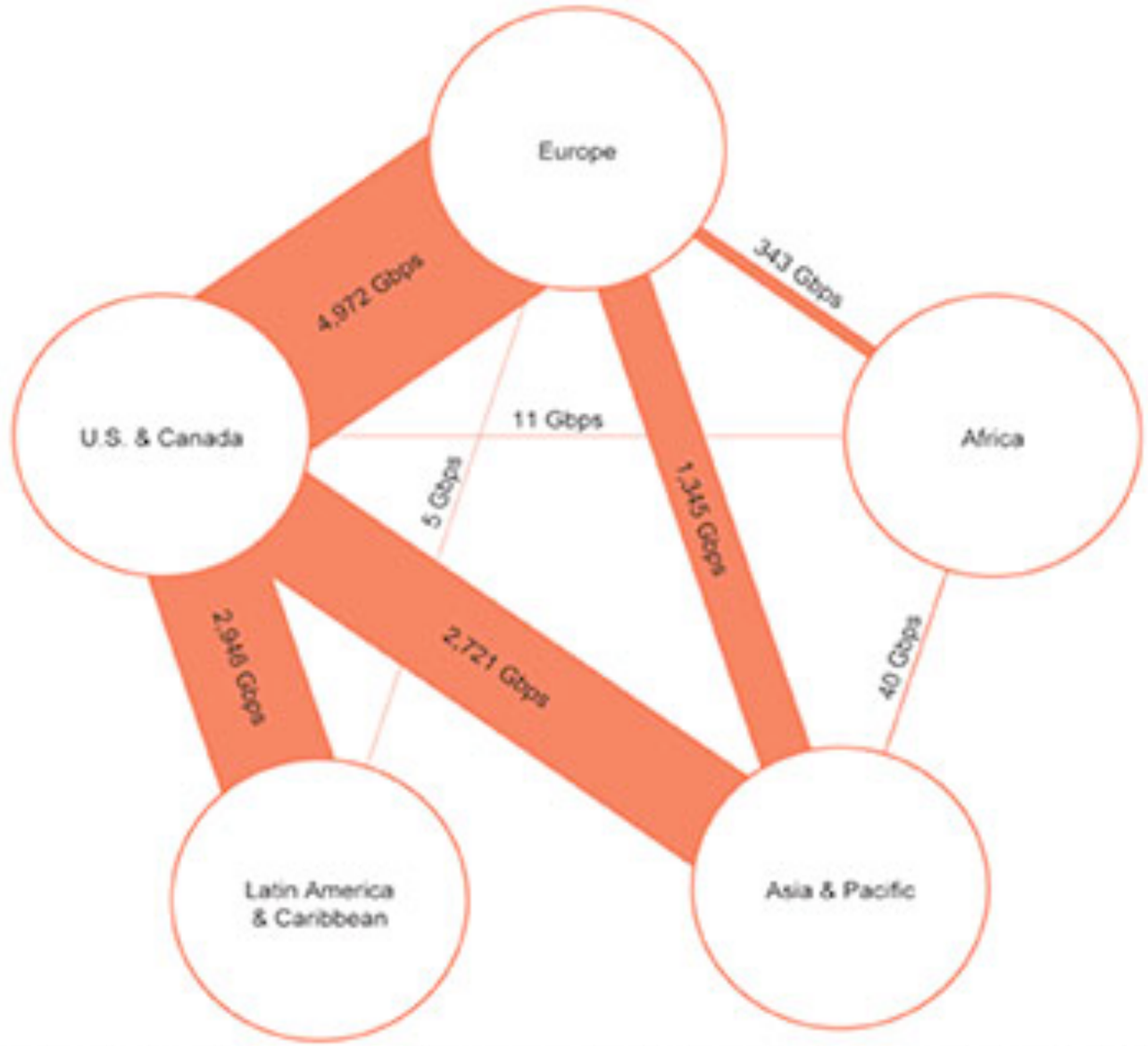
[redacted]

April 2013

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

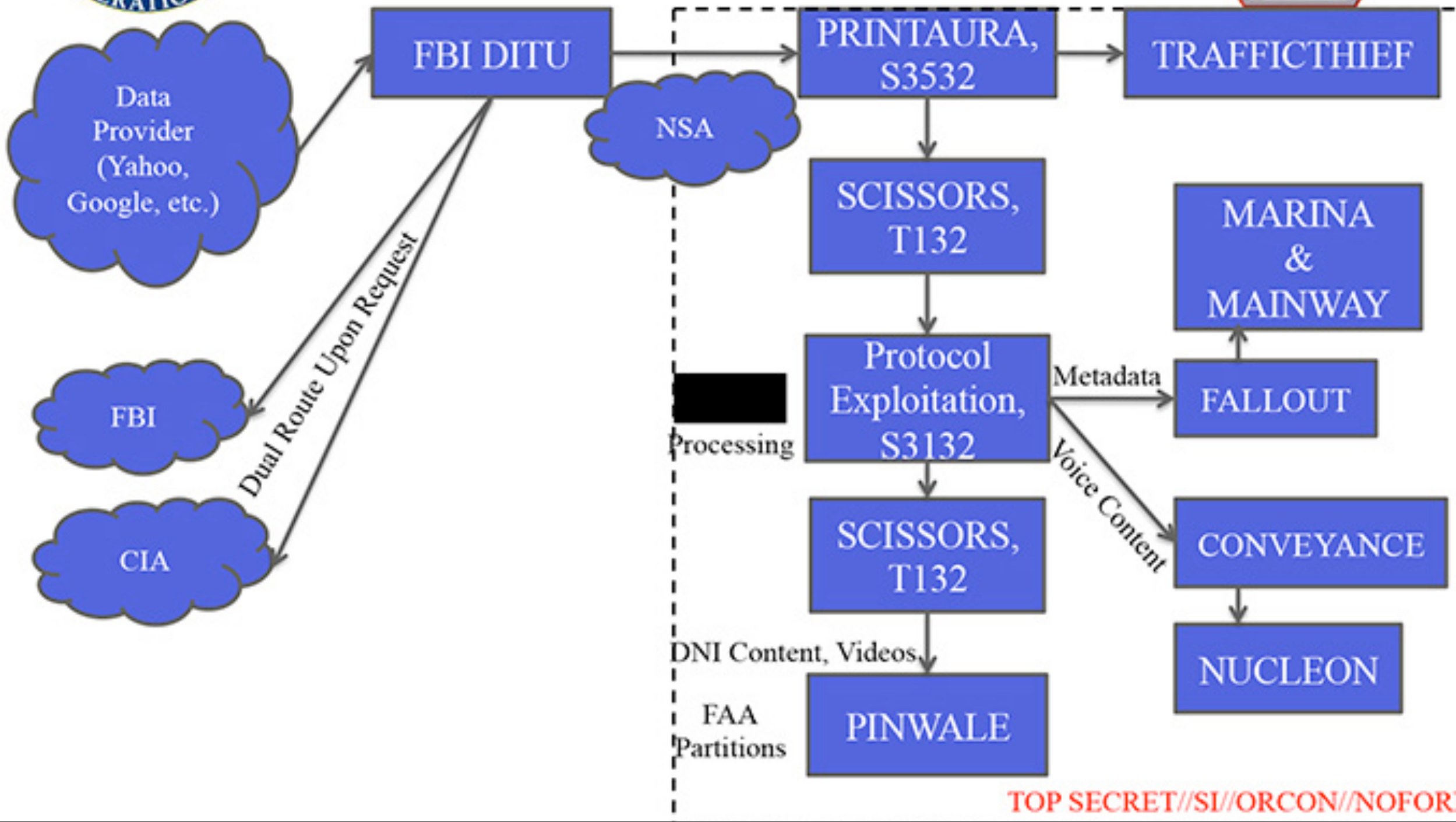


International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

(TS//SI//NF) PRISM Tasking Process

(TS//SI//NF) PRISM Collection Dataflow



(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
- P1: Microsoft
- P2: Yahoo
- P3: Google
- P4: Facebook
- P5: PalTalk
- P6: YouTube
- P7: Skype
- P8: AOL
- PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
- A: Stored Comms (Search)
- B: IM (chat)
- C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
- D: RTN-IM (real-time notification of a chat login or logout event)
- E: E-Mail
- F: VoIP
- G: Full (WebForum)
- H: OSN Messaging (photos, wallposts, activity, etc.)
- I: OSN Basic Subscriber Info
- J: Videos
- . (dot): Indicates multiple types

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

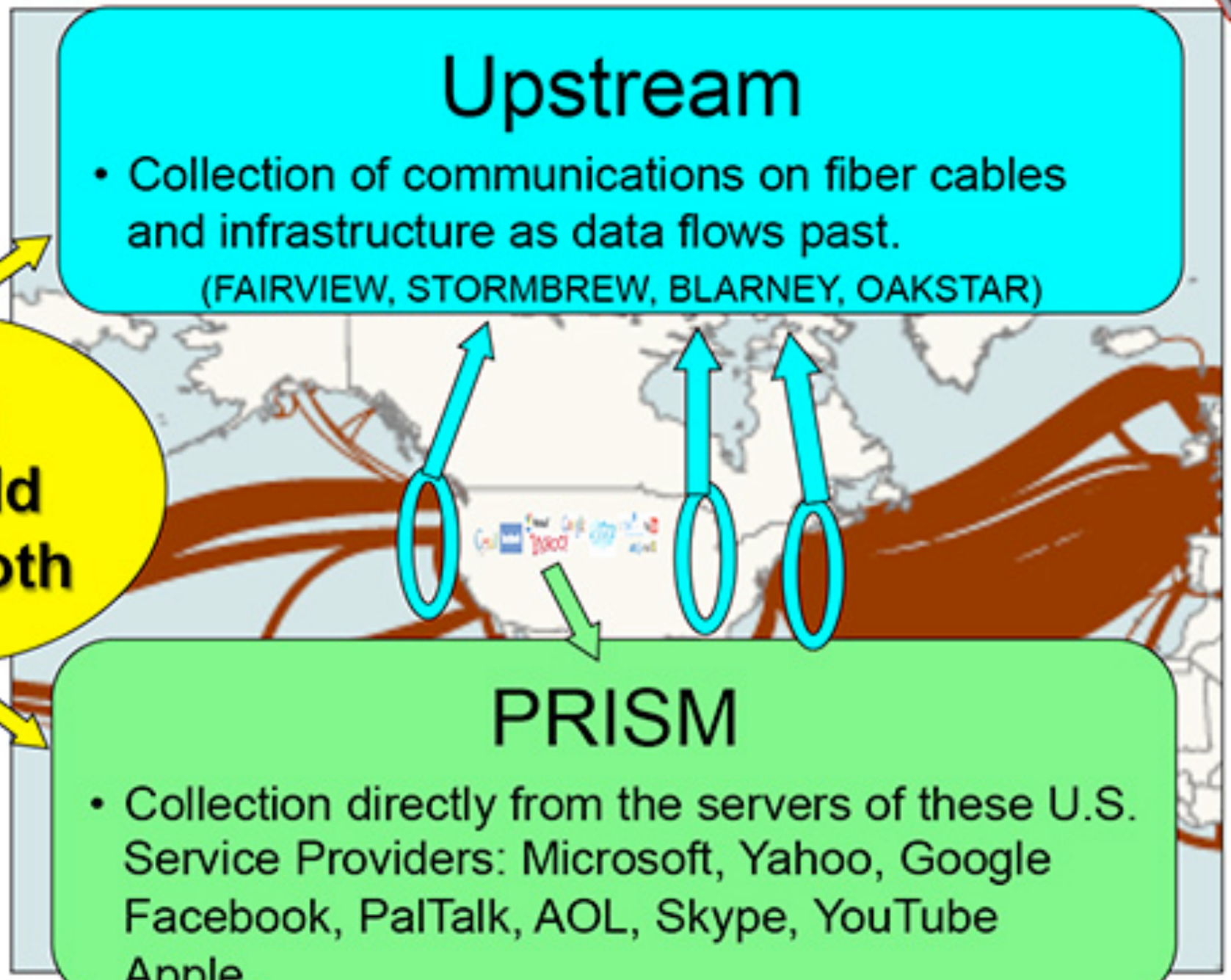
Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.
  (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

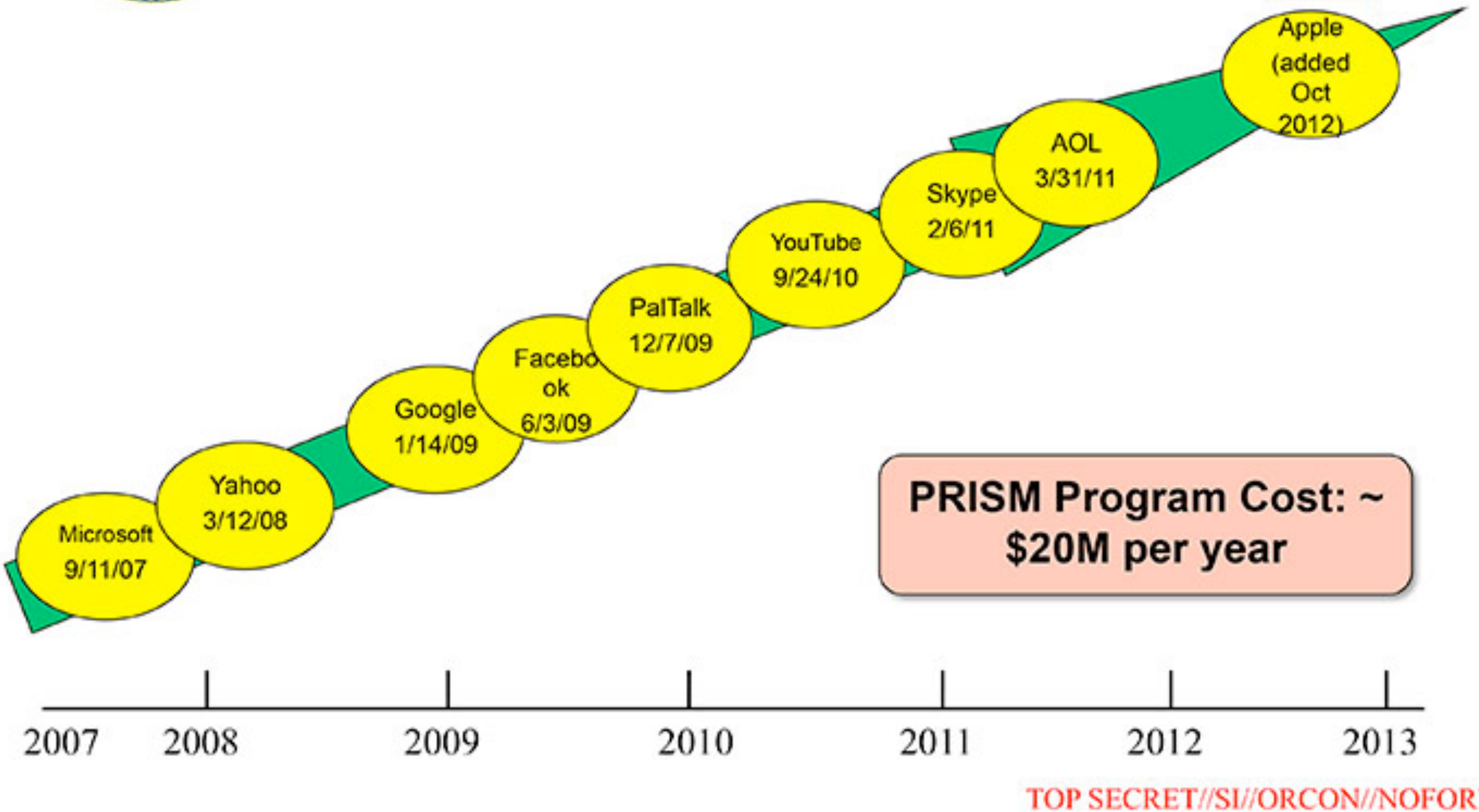


You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) REPRISMFISA TIPS

(https:/[redacted]

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET/[redacted]/SI/TK//ORCON/NOFORN

REPRISMFISA

COUNTERTERRORISM

[redacted] 2013-Apr-05 13:10:28Z

Click on the PRISM icon first (from the initial webpage)

PRISM FBI FISA DOJ FISA

PRISM ENTRIES

Last Load on Apr 05, 2013 at 12:22 PM GMT

Check the total record status, click on this link

QUICK LINKS

- See Entire List (Current)
- See Entire List (Expired)
- See Entire List (Current and Expired)
- See NSA List
- See New Records
- Ownership Count

If the total count is much less than this, REPRISMFISA is having issues, E-MAIL the REPRISMFISA HELP DESK AT [redacted] AND INFORM THEM

SEARCH

The search form below can be used as a filter to see a partial list of records.

Search For:

AND OR

Expiration days (+/- from now)

Filter

Prism Current Entries

Records 1 - 50 out of 117675 << < Page 1 of 2354 > >> Records per page: 50

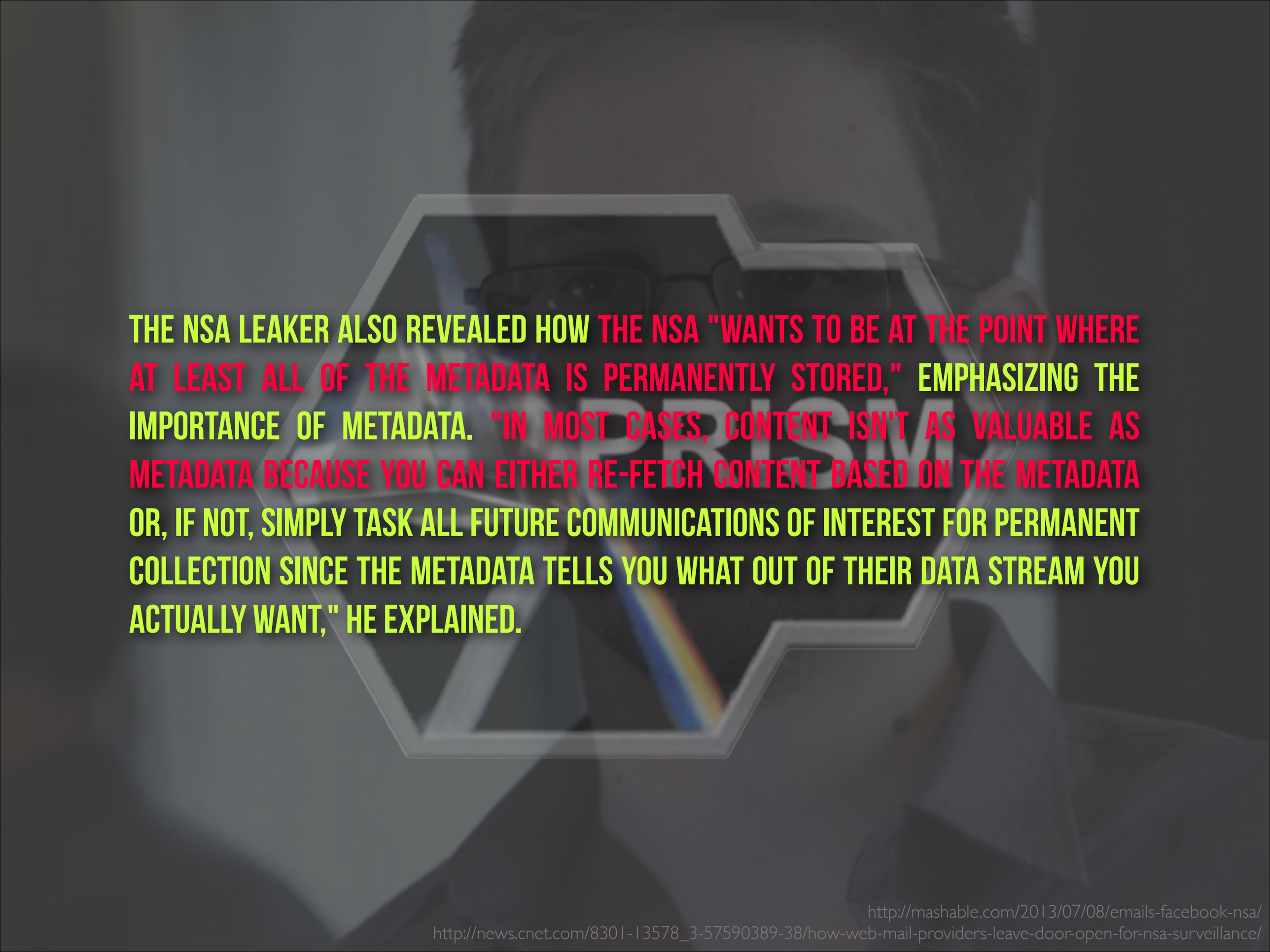
Clear Sort Order Click on column headers to sort. * = column is not sortable.

https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

IN THE LENGTHY Q&A CARRIED OUT OVER ENCRYPTED EMAILS, SNOWDEN SAID THAT ONE CAN BE TARGETED BECAUSE OF HIS HER EMAILS AND FACEBOOK PROFILE, BUT DIDN'T INCLUDE ANY PRECISE DETAILS OF THE INNER WORKINGS. WHEN ASKED WHAT HAPPENS TO TARGETS, THOUGH, HE REVEALED A BIT MORE.

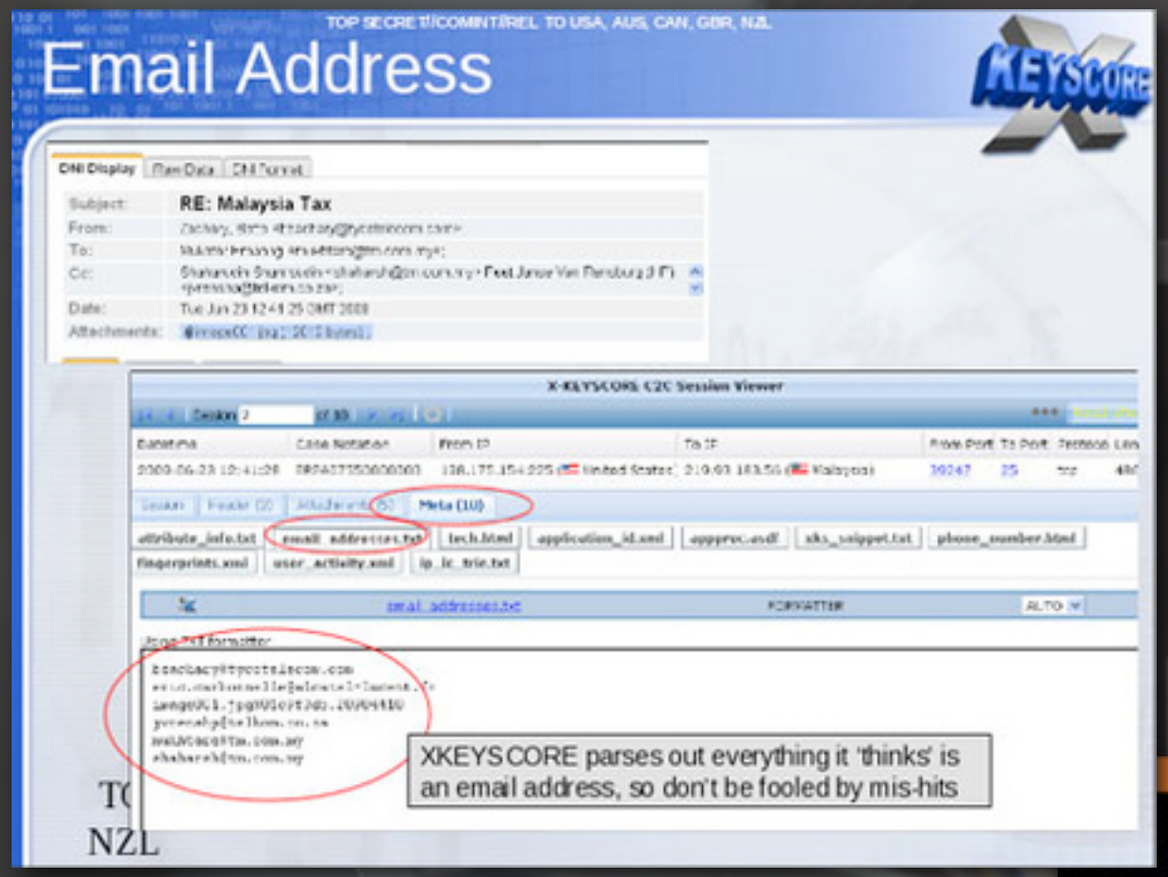
"THEY'RE JUST OWNED. AN ANALYST WILL GET A DAILY (OR SCHEDULED BASED ON EXFILTRATION SUMMARY) REPORT ON WHAT CHANGED ON THE SYSTEM, PCAPS [ABBREVIATION OF THE TERM "PACKET CAPTURE"] OF LEFTOVER DATA THAT WASN'T UNDERSTOOD BY THE AUTOMATED DISSECTORS, AND SO FORTH," SNOWDEN WROTE. "

http://mashable.com/2013/07/08/emails-facebook-nsa/
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/



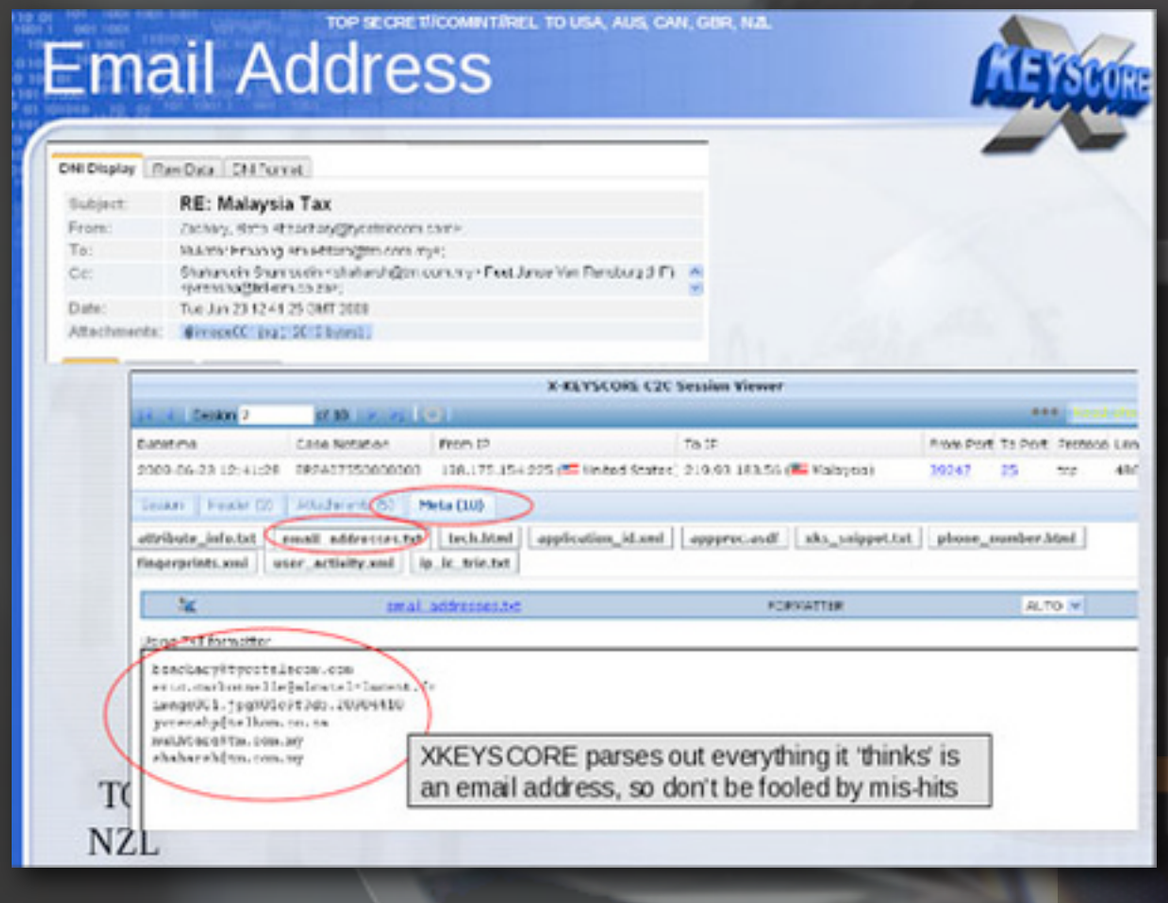
THE NSA LEAKER ALSO REVEALED HOW THE NSA "WANTS TO BE AT THE POINT WHERE AT LEAST ALL OF THE METADATA IS PERMANENTLY STORED," EMPHASIZING THE IMPORTANCE OF METADATA. "IN MOST CASES, CONTENT ISN'T AS VALUABLE AS METADATA BECAUSE YOU CAN EITHER RE-FETCH CONTENT BASED ON THE METADATA OR, IF NOT, SIMPLY TASK ALL FUTURE COMMUNICATIONS OF INTEREST FOR PERMANENT COLLECTION SINCE THE METADATA TELLS YOU WHAT OUT OF THEIR DATA STREAM YOU ACTUALLY WANT," HE EXPLAINED.

http://mashable.com/2013/07/08/emails-facebook-nsa/
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/



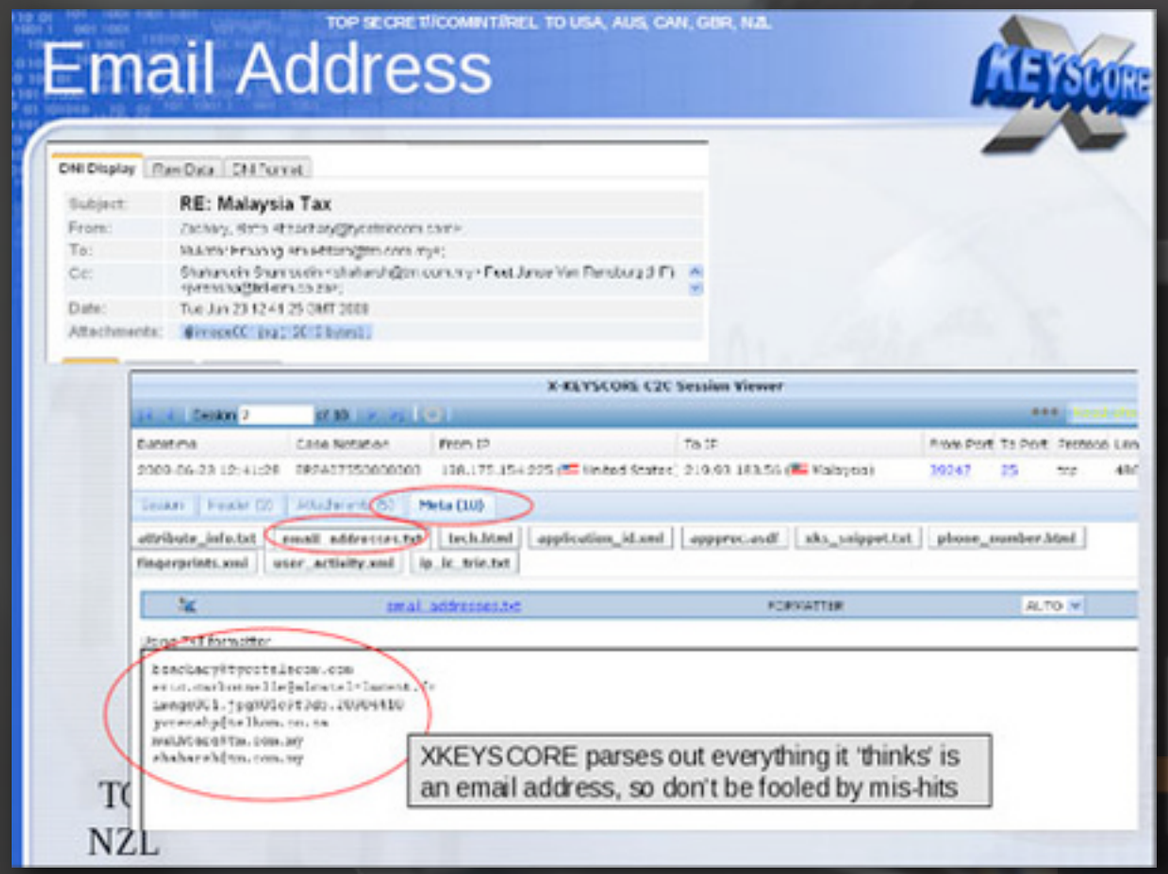
XKEYSCORE

http://www.theverge.com/2013/7/31/4574532/xkeyscore-data-tracking-program-detailed-in-documents



CENTRAL INTERFACE FOR EMAIL, FACEBOOK CHAT, WEB BROWSING HISTORY, AND MORE. [...] ITS VAST DATABASE ALLOWS USERS TO FIND PEOPLE BY EMAIL ADDRESS, NAME, PHONE NUMBER, TYPE OF BROWSER, LANGUAGE USED, IP ADDRESS, OR SPECIFIC KEYWORDS.

http://www.theverge.com/2013/7/31/4574532/xkeyscore-data-tracking-program-detailed-in-documents



RISM

Why are we interested in HTTP?

THE GUARDIAN REPORTS THAT IN 2012, 41 BILLION INDIVIDUAL RECORDS WERE STORED IN XKEYSCORE OVER ONE THIRTY-DAY PERIOD. ACTUAL CONTENT LIKE EMAIL TEXT IS ALSO INCLUDED IN THE DATABASE. [....] EMAILS STORED FOR ONLY THREE TO FIVE DAYS, WITH METADATA STORED FOR THIRTY DAYS. IF CONTENT IS DEEMED "INTERESTING," THOUGH, IT'S MOVED TO OTHER DATABASES, WHERE IT CAN BE STORED FOR UP TO FIVE YEARS.

http://www.theverge.com/2013/7/31/4574532/xkeyscore-data-tracking-program-detailed-in-documents

THE NSA ISN'T THE ONLY SURVEILLANCE POWER THAT NETIZENS SHOULD BE WORRIED ABOUT. SNOWDEN EXPLAINED IN THE INTERVIEW THAT ITS ALLIED COUNTERPARTS FROM THE UK, AUSTRALIA, NEW ZEALAND AND CANADA — PART OF THE SO-CALLED FIVE-EYES — "GO BEYOND WHAT NSA ITSELF DOES."

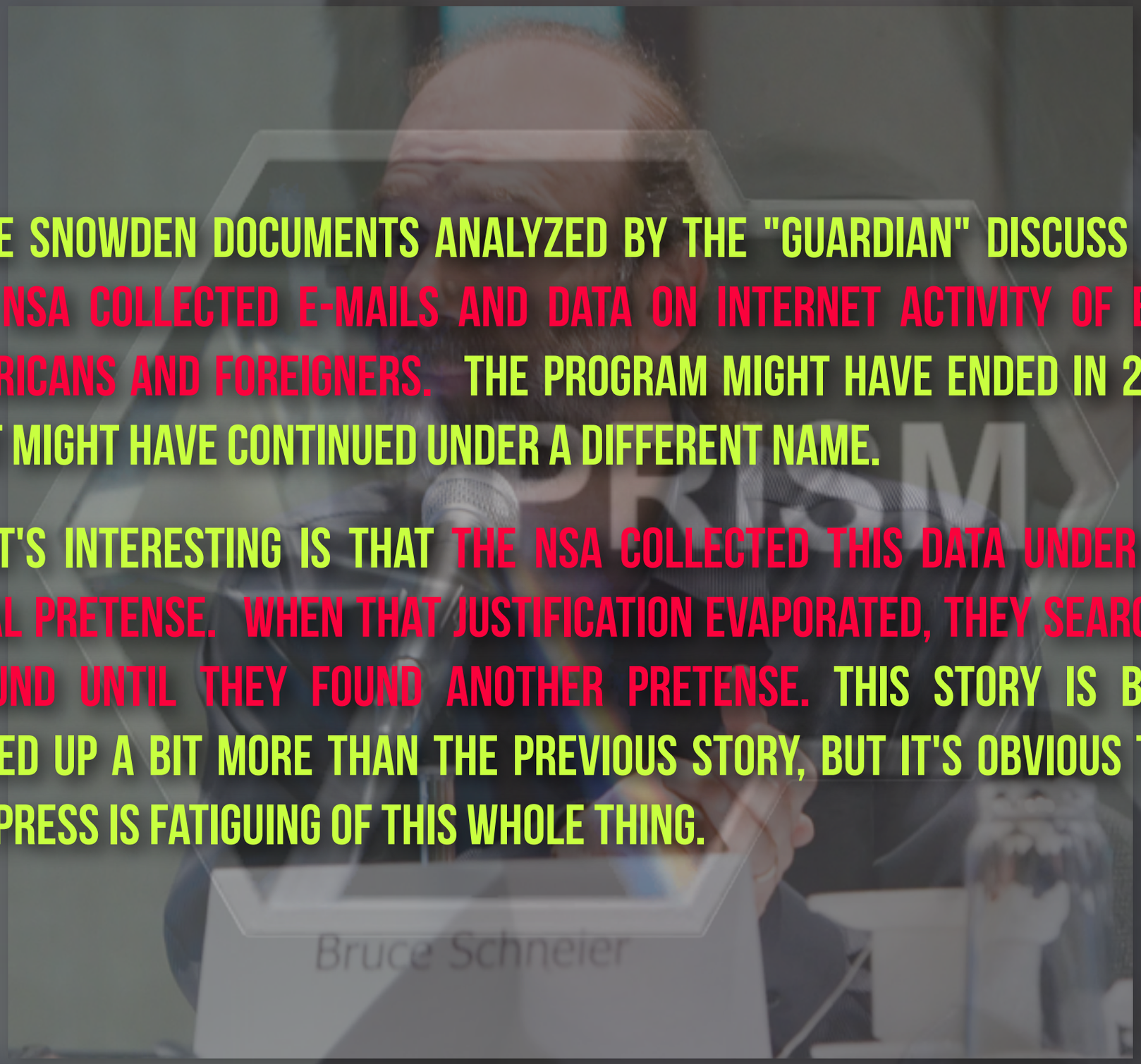
THE BRITISH SPY AGENCY GCHQ SECRETLY TAPS FIBER-OPTIC CABLES THROUGH A SURVEILLANCE PROGRAM CALLED PROJECT TEMPORA, A REPORT IN THE GUARDIAN REVEALED. THAT PROCEDURE "SNARFS EVERYTHING, IN A ROLLING BUFFER TO ALLOW RETROACTIVE INVESTIGATION WITHOUT MISSING A SINGLE BIT," SNOWDEN WROTE. "IF YOU SEND A SINGLE ICMP PACKET 5 [REFERRING TO ALL DATA PACKETS SENT TO OR FROM BRITAIN] AND IT ROUTES THROUGH THE UK, WE GET IT.

http://mashable.com/2013/07/08/emails-facebook-nsa/
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

https://www.schneier.com/blog/archives/2013/07/nsa_e-mail_eave.html
https://secure.flickr.com/photos/villoks/492857088/sizes/l/in/photostream/
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

MORE SNOWDEN DOCUMENTS ANALYZED BY THE "GUARDIAN" DISCUSS HOW THE NSA COLLECTED E-MAILS AND DATA ON INTERNET ACTIVITY OF BOTH AMERICANS AND FOREIGNERS. THE PROGRAM MIGHT HAVE ENDED IN 2011, OR IT MIGHT HAVE CONTINUED UNDER A DIFFERENT NAME.

WHAT'S INTERESTING IS THAT THE NSA COLLECTED THIS DATA UNDER ONE LEGAL PRETENSE. WHEN THAT JUSTIFICATION EVAPORATED, THEY SEARCHED AROUND UNTIL THEY FOUND ANOTHER PRETENSE. THIS STORY IS BEING PICKED UP A BIT MORE THAN THE PREVIOUS STORY, BUT IT'S OBVIOUS THAT THE PRESS IS FATIGUING OF THIS WHOLE THING.



https://www.schneier.com/blog/archives/2013/07/nsa_e-mail_eave.html
https://secure.flickr.com/photos/villoks/492857088/sizes/l/in/photostream/
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

(MEANWHILE) WEB MAIL PROVIDERS LEAVE DOOR OPEN FOR NSA SURVEILLANCE

PROTECTING USERS' E-MAIL PRIVACY FROM THE NATIONAL SECURITY AGENCY AND OTHER INTELLIGENCE SERVICES MEANS USING ENCRYPTION. BUT WITH THE EXCEPTION OF GOOGLE, FEW COMPANIES DO EVERYTHING THEY CAN.

(INITIAL) SECURITY IS PROVIDED VIA HTTPS - BUT DURING THE NEXT STEP, WHEN THOSE E-MAIL MESSAGES ARE TRANSFERRED FROM ONE COMPANY'S SERVERS TO ANOTHER'S, THEY'RE RARELY ENCRYPTED. AN E-MAIL MESSAGE THAT A FACEBOOK USER ADDRESSES TO A YAHOO MAIL USER, FOR INSTANCE, WILL BE DELIVERED IN AN UNENCRYPTED FORM THROUGH A SERVER-TO-SERVER CONNECTION THAT PROVIDES NO PROTECTION AGAINST SURVEILLANCE.

http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/
https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

US webmail providers supporting server-to-server encryption (tls)

Gmail by Google = YES?

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
gmail-smtp-in.l.google.com [173.194.74.26]	5	OK (31ms)	OK (28ms)	OK (204ms)	OK (30ms)	FAIL	OK (563ms)	OK (43ms)	OK (786ms)
alt1.gmail-smtp-in.l.google.com [173.194.66.26]	10	OK (103ms)	OK (102ms)	OK (410ms)	OK (105ms)	FAIL	OK (1,619ms)	OK (1,384ms)	OK (528ms)
alt2.gmail-smtp-in.l.google.com [74.125.136.26]	20	OK (583ms)	OK (101ms)	OK (103ms)	OK (103ms)	FAIL	OK (1,325ms)	OK (102ms)	OK (540ms)
alt3.gmail-smtp-in.l.google.com [173.194.70.26]	30	OK (105ms)	OK (114ms)	OK (119ms)	OK (118ms)	FAIL	OK (924ms)	OK (428ms)	OK (562ms)
alt4.gmail-smtp-in.l.google.com [173.194.69.26]	40	OK (111ms)	OK (110ms)	OK (113ms)	OK (112ms)	FAIL	OK (1,356ms)	OK (112ms)	OK (491ms)
Average		100%	100%	100%	100%	0%	100%	100%	100%

Microsoft Hotmail = NO!

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
mx2.hotmail.com [65.55.92.152]	5	OK (81ms)	OK (659ms)	OK (353ms)	FAIL	FAIL	FAIL	OK (1,346ms)	OK (611ms)
mx3.hotmail.com [65.54.188.72]	5	OK (79ms)	OK (273ms)	OK (267ms)	FAIL	FAIL	FAIL	OK (951ms)	OK (293ms)
mx4.hotmail.com [65.55.37.104]	5	OK (81ms)	OK (292ms)	OK (295ms)	FAIL	FAIL	FAIL	OK (1,146ms)	OK (455ms)
mx1.hotmail.com [65.55.92.168]	5	OK (290ms)	OK (77ms)	OK (291ms)	FAIL	FAIL	FAIL	OK (901ms)	OK (246ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

YAHOO! = NO!

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
mta7.am0.yahoodns.net [98.136.217.203]	1	OK (78ms)	OK (77ms)	OK (76ms)	FAIL	FAIL	FAIL	OK (439ms)	OK (75ms)
mta6.am0.yahoodns.net [98.136.216.25]	1	OK (83ms)	OK (85ms)	OK (197ms)	FAIL	FAIL	FAIL	OK (448ms)	OK (345ms)
mta5.am0.yahoodns.net [98.136.216.26]	1	OK (775ms)	OK (51ms)	OK (52ms)	FAIL	FAIL	FAIL	OK (1,442ms)	OK (51ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

AOL = NO!

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
mailin-01.mx.aol.com [64.12.90.98]	15	OK (27ms)	OK (185ms)	OK (76ms)	FAIL	FAIL	FAIL	OK (693ms)	OK (34ms)
mailin-02.mx.aol.com [64.12.90.65]	15	OK (27ms)	OK (261ms)	OK (31ms)	FAIL	FAIL	FAIL	OK (512ms)	OK (32ms)
mailin-03.mx.aol.com [205.188.190.2]	15	OK (114ms)	OK (295ms)	OK (29ms)	FAIL	FAIL	FAIL	OK (632ms)	OK (32ms)
mailin-04.mx.aol.com [205.188.146.194]	15	OK (26ms)	OK (231ms)	OK (30ms)	FAIL	FAIL	FAIL	OK (328ms)	OK (171ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

(emails between these services can be monitored)

by: ashk4n - 06/17/2013 - using http://www.checktls.com/

http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

https://secure.flickr.com/photos/98137931@N02/9161328604/s

https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

BILLIONS OF SUPPOSEDLY PRIVATE E-MAIL MESSAGES A DAY FLOW THROUGH UNSECURED LINKS, (LACKING SMTP-TLS) WHERE THEY CAN BE SNARED IN DIGITAL DRAGNETS OPERATED BY THE NATIONAL SECURITY AGENCY AND OTHER INTELLIGENCE SERVICES.

SNOWDEN SAID [...] "AMERICANS' COMMUNICATIONS ARE COLLECTED AND VIEWED ON A DAILY BASIS ON THE CERTIFICATION OF AN ANALYST RATHER THAN A WARRANT."

http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/
https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

A LEAKED NSA SLIDE TALKING ABOUT "UPSTREAM" DATA COLLECTION FROM "FIBER CABLES AND INFRASTRUCTURE AS DATA FLOWS PAST" SUGGESTS THAT THOSE COMPANIES ARE TELLING THE TRUTH: THE NSA INSTEAD IS TAPPING INTO INTERNET BACKBONE LINKS OPERATED BY COMPANIES SUCH AS AT&T, CENTURYLINK, XO COMMUNICATIONS, VERIZON, AND LEVEL 3 COMMUNICATIONS -- AND USING THAT PASSIVE ACCESS TO VACUUM UP UNENCRYPTED COMMUNICATIONS. ADDITIONAL EVIDENCE COMES FROM THE CLASSIFIED DIRECTIVES RELEASED THURSDAY THAT DISCUSS SURVEILLANCE PROCEDURES AND WERE SIGNED BY ATTORNEY GENERAL ERIC HOLDER.

http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/
https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

https://secure.flickr.com/photos/98137931@N02/9161328604/s
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama l
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

THE OBAMA ADMINISTRATION HAD ALLOWED FOR THE CONTINUATION OF AN NSA DATA COLLECTION PROGRAM FOR TWO YEARS STARTED DURING PRESIDENT GEORGE W. BUSH'S FIRST MANDATE IN 2001.

https://www.net-security.org/secworld.php?id=15159
http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/

http://www.mattbors.com/blog/2013/06/27/spy-vs-spy/
https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

https://secure.flickr.com/photos/98137931@N02/9161328604/sizes/o/

THE NSA

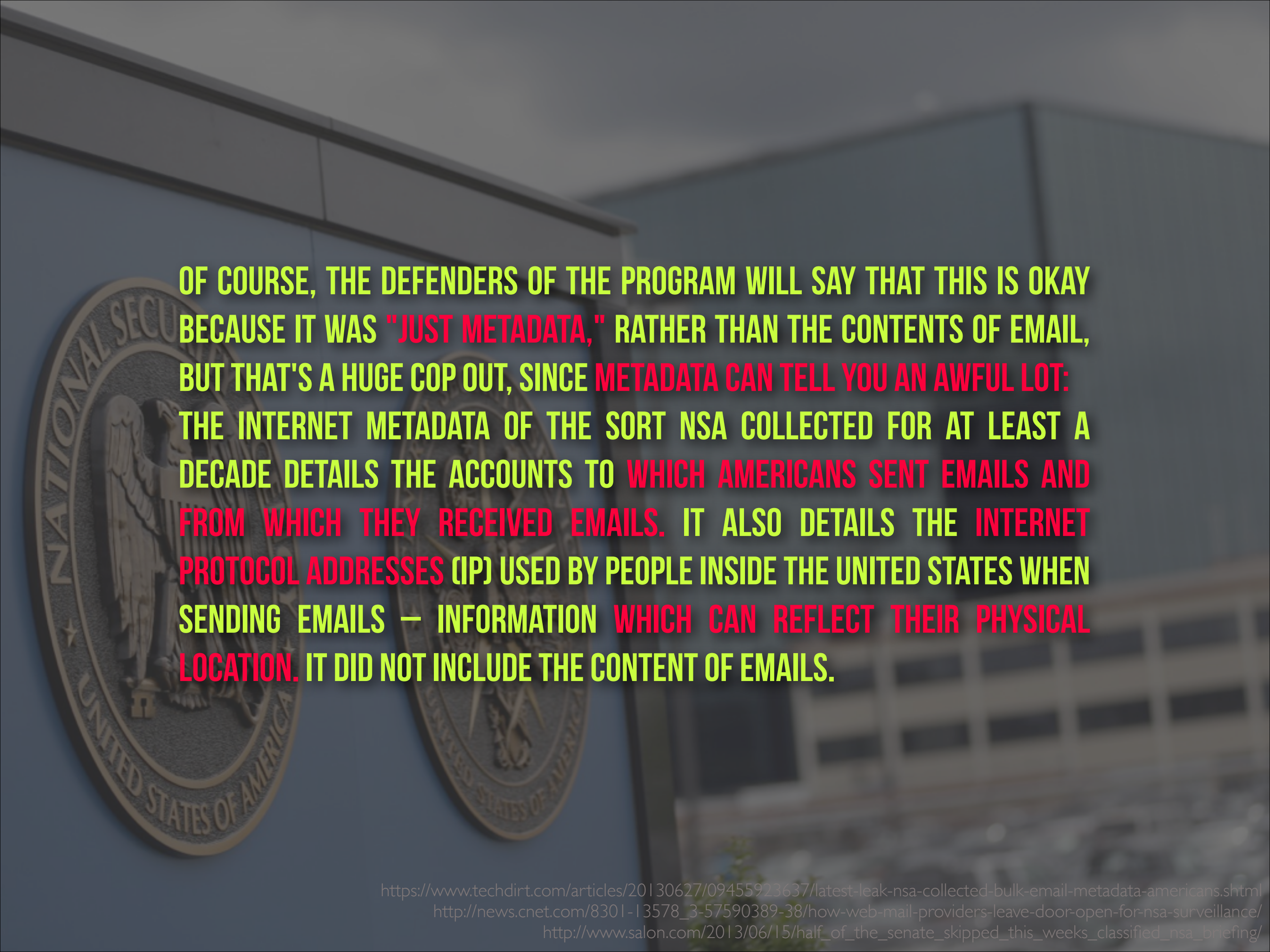
http://www.sa[illegible]/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

THE NSA LEAKS JUST KEEP ON COMING, AND THE LATEST ONE IS A BIG ONE. IT'S CONCERNING THE NSA IS ABOUT THE STELLAR WIND PROGRAM -- WHICH HAD BEEN REVEALED BEFORE, AND WHICH FORMER NSA WHISTLEBLOWER BILL BINNEY HAS DISCUSSED IN THE PAST -- BUT BINNEY LEFT THE NSA IN 2001. THE LATEST DOCUMENT IS A REPORT FROM THE INSPECTOR GENERAL THAT CONFIRMS SOME OF THE CLAIMS BINNEY HAS MADE IN THE PAST.

EVENTUALLY, THE NSA GAINED AUTHORITY TO "ANALYZE COMMUNICATIONS METADATA ASSOCIATED WITH UNITED STATES PERSONS AND PERSONS BELIEVED TO BE IN THE UNITED STATES", ACCORDING TO A 2007 JUSTICE DEPARTMENT MEMO, WHICH IS MARKED SECRET.

SO, REMEMBER ALL THAT STUFF THE NSA [...] SAYING ABOUT HOW THEY'RE NOT COLLECTING INTERNET DATA ON AMERICANS? AND HOW THEY HAVE MINIMIZATION PROCEDURES AND ALL OF THAT?

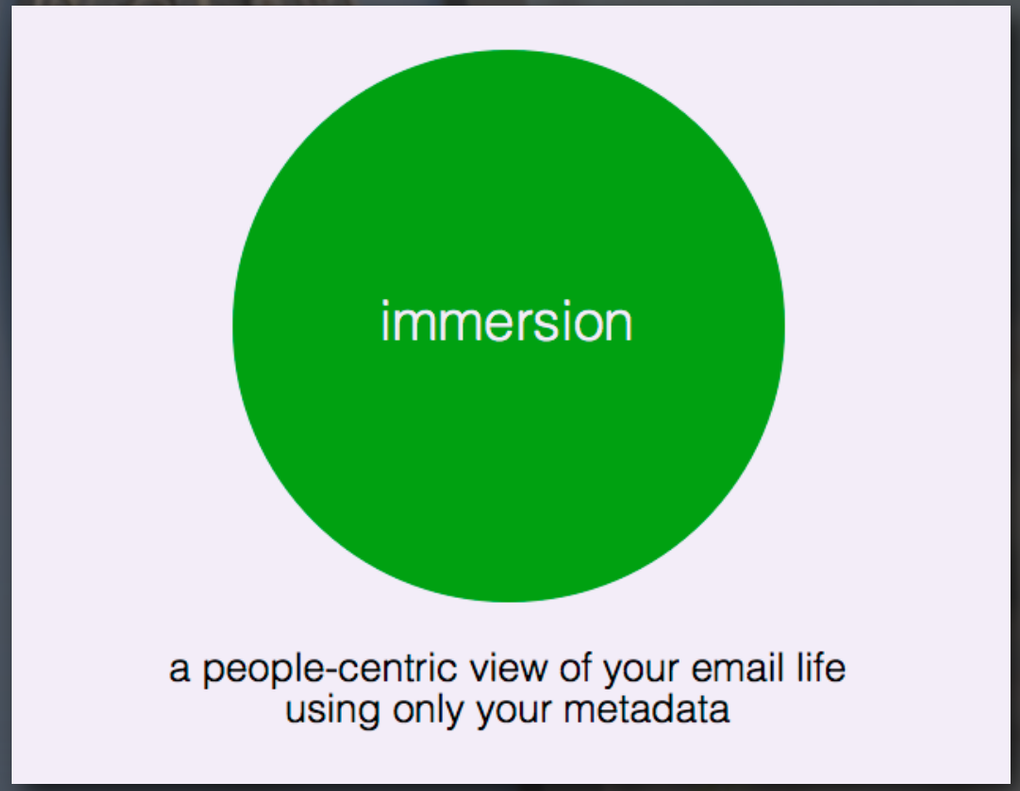
https://www.techdirt.com/articles/20130627/09455923637/latest-leak-nsa-collected-bulk-email-metadata-americans.shtml
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/



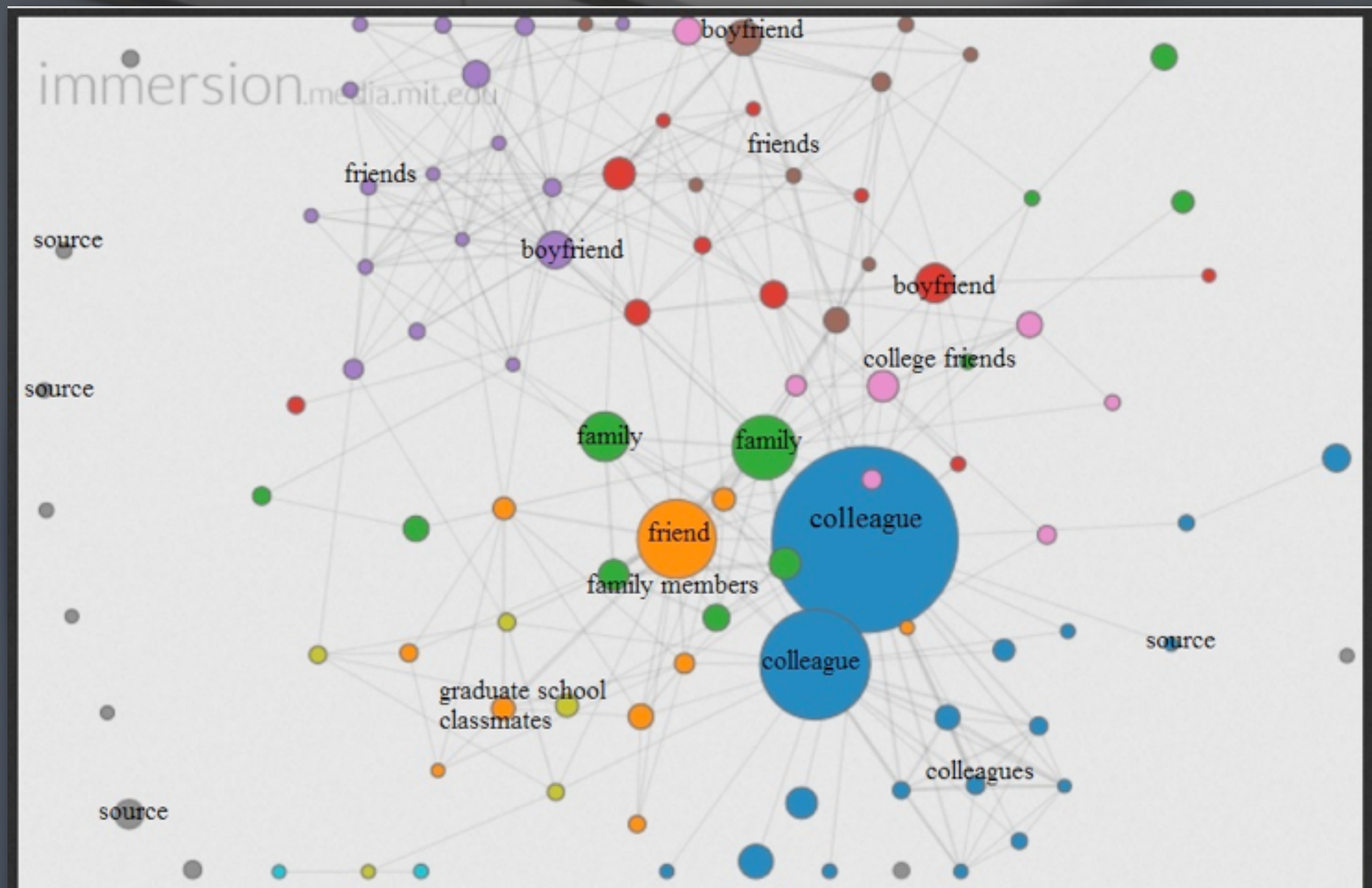
OF COURSE, THE DEFENDERS OF THE PROGRAM WILL SAY THAT THIS IS OKAY BECAUSE IT WAS "JUST METADATA," RATHER THAN THE CONTENTS OF EMAIL, BUT THAT'S A HUGE COP OUT, SINCE METADATA CAN TELL YOU AN AWFUL LOT: THE INTERNET METADATA OF THE SORT NSA COLLECTED FOR AT LEAST A DECADE DETAILS THE ACCOUNTS TO WHICH AMERICANS SENT EMAILS AND FROM WHICH THEY RECEIVED EMAILS. IT ALSO DETAILS THE INTERNET PROTOCOL ADDRESSES (IP) USED BY PEOPLE INSIDE THE UNITED STATES WHEN SENDING EMAILS – INFORMATION WHICH CAN REFLECT THEIR PHYSICAL LOCATION. IT DID NOT INCLUDE THE CONTENT OF EMAILS.

https://www.techdirt.com/articles/20130627/09455923637/latest-leak-nsa-collected-bulk-email-metadata-americans.shtml
http://news.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

MIT MEDIA LAB HAS DEVELOPED A NEW ONLINE PROJECT, CALLED IMMERSION, WHICH TAKES YOUR GMAIL METADATA AND TURNS IT INTO A MAP LINKING TOGETHER PEOPLE IN YOUR LIFE.



\http://www.t3.com/news/mit-tool-uses-gmail-metadata-to-give-you-a-people-centric-view-of-your-email-life
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/



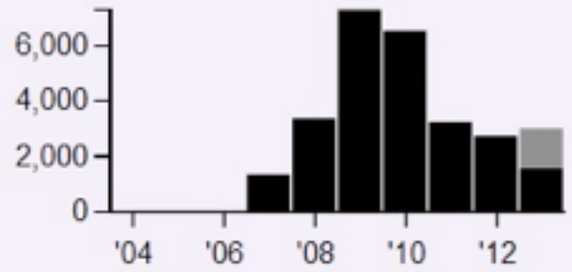
Kashmir Hill

916 collaborators

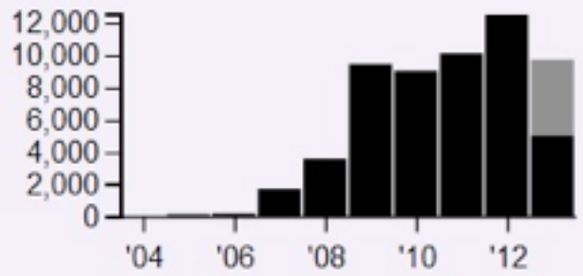
78,277 emails

My Stats | Top Collaborators

Emails Sent



Emails Received



http://www.forbes.com/sites/kashmirhill/2013/07/10/heres-a-tool-to-see-what-your-email-metadata-reveals-about-you/

http://www.t3.com/news/new-tool-uses-gmail-metadata-to-give-you-a-people-centric-view-of-your-email-life

http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing

HIDALGO GOES ON TO EXPRESS THAT FOR HIM, METADATA IS AN EMOTIONAL ISSUE. A USERS METADATA IS ALL ABOUT INTERACTIONS BETWEEN PEOPLE AND THOSE INTERACTIONS ARE ASSOCIATED WITH OUR EMOTIONS.

http://www.forbes.com/sites/kashmirhill/2013/07/10/heres-a-tool-to-see-what-your-email-metadata-reveals-about-you/
http://www.t3.com/news/this-tool-uses-gmail-metadata-to-give-you-a-people-centric-view-of-your-email-life
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing

IF DATA IS ENCRYPTED, YOU MIGHT BE EVIL, SO WE'LL KEEP IT UNTIL WE'RE SURE FROM THE SAY-WHAT-NOW? DEPT

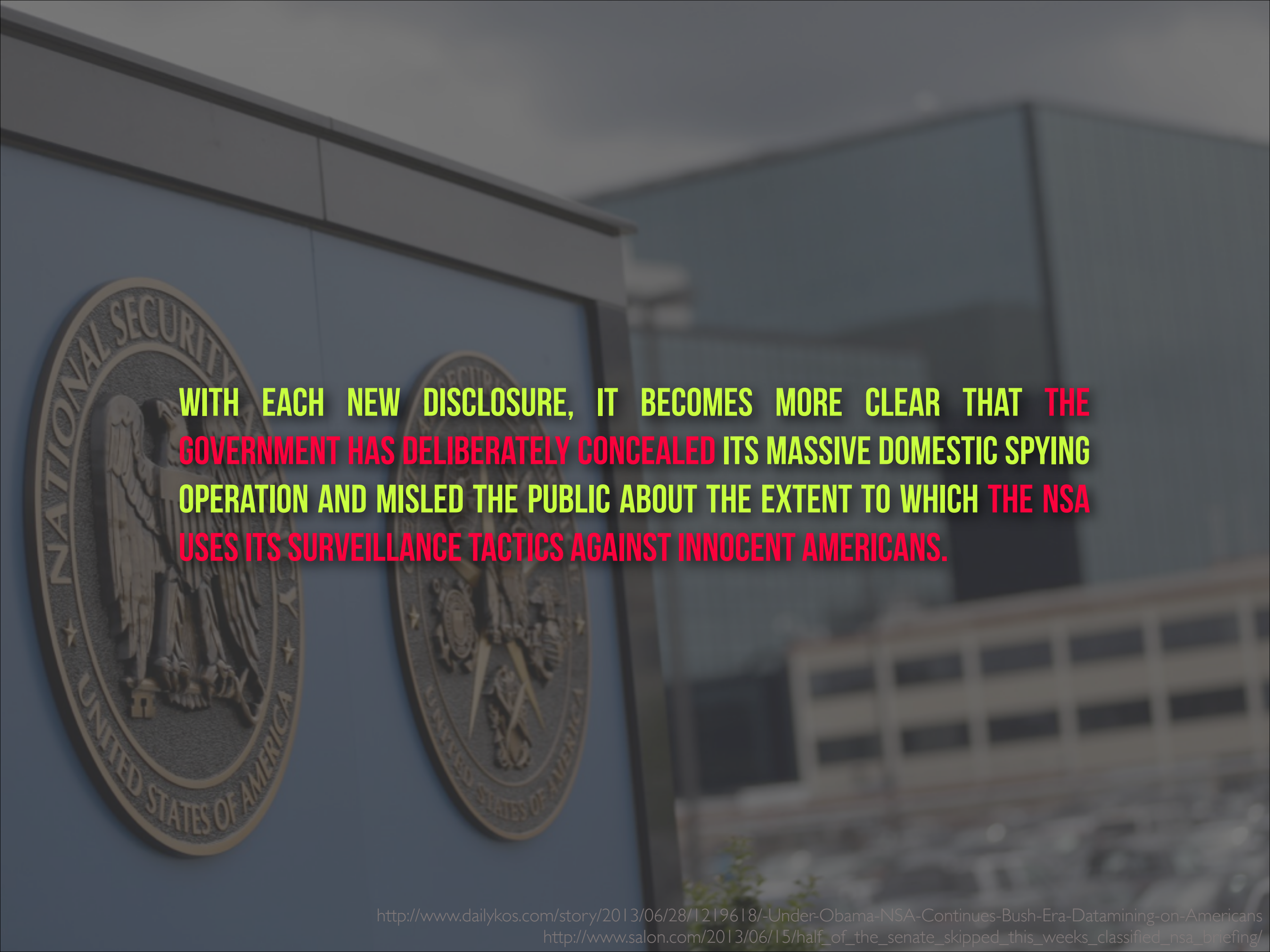
IN THE CONTEXT OF A CRYPTANALYTIC EFFORT, MAINTENANCE OF TECHNICAL DATA BASES REQUIRES RETENTION OF ALL COMMUNICATIONS THAT ARE ENCIPHERED OR REASONABLY BELIEVED TO CONTAIN SECRET MEANING, AND SUFFICIENT DURATION MAY CONSIST OF ANY PERIOD OF TIME DURING WHICH ENCRYPTED MATERIAL IS SUBJECT TO, OR OF USE IN, CRYPTANALYSIS. THE DEFAULT IS IF THE NSA ISN'T SURE ABOUT ANYTHING, IT CAN KEEP YOUR DATA.

https://www.techdirt.com/articles/20130620/15390323549/nsa-has-convinced-fisa-court-that-if-your-data-is-encrypted-you-might-be-terrorist-so-itll-hang-onto-your-data.shtml
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

IF IT DISCOVERS ANYTHING AT ALL REMOTELY POTENTIALLY CRIMINAL ABOUT YOUR DATA, IT CAN KEEP IT, EVEN IF IT DIDN'T COLLECT IT FOR THAT PURPOSE. AS KEVIN BANKSTON POINTS OUT TO ANDY GREENBERG IN THE LINK ABOVE:

THE DEFAULT IS THAT YOUR COMMUNICATIONS ARE UNPROTECTED. THAT'S THE EXACT OPPOSITE OF HOW IT'S SUPPOSED TO BE UNDER THE CONSTITUTION. THE DEFAULT IS SUPPOSED TO BE THAT YOUR COMMUNICATIONS ARE PROTECTED, AND IF THE GOVERNMENT WANTS TO SEE IT, IT NEEDS TO GO TO COURT TO GET A SPECIFIC WARRANT FOR THAT INFORMATION.

https://www.techdirt.com/articles/20130620/15390323549/nsa-has-convinced-fisa-court-that-if-your-data-is-encrypted-you-might-be-terrorist-so-itll-hang-onto-your-data.shtml
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

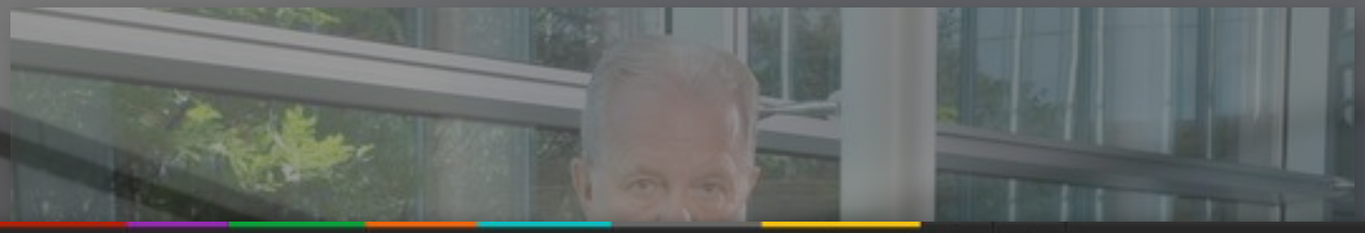


WITH EACH NEW DISCLOSURE, IT BECOMES MORE CLEAR THAT THE GOVERNMENT HAS DELIBERATELY CONCEALED ITS MASSIVE DOMESTIC SPYING OPERATION AND MISLED THE PUBLIC ABOUT THE EXTENT TO WHICH THE NSA USES ITS SURVEILLANCE TACTICS AGAINST INNOCENT AMERICANS.

http://www.dailykos.com/story/2013/06/28/1219618/-Under-Obama-NSA-Continues-Bush-Era-Datamining-on-Americans
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

IT IS THANKS TO WHISTLEBLOWERS LIKE THOMAS DRAKE, WILLIAM BINNEY, KIRK WIEBE, AND SNOWDEN THAT THE PUBLIC CAN NOW HAVE A MORE OPEN DEBATE ABOUT THE WISDOM AND EFFICACY OF THESE SPYING POWERS AND THAT THE COURTS AND CONGRESS ARE AFFORDED AN OPPORTUNITY TO ENGAGE IN MORE AGGRESSIVE AND BADLY NEEDED OVERSIGHT.

http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/
http://www.dailykos.com/story/2013/06/28/1219618/-Under-Obama-NSA-Continues-Bush-Era-Datamining-on-Americans
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/



USA TODAY | NEWS | SPORTS | LIFE | MONEY | TECH | TRAVEL | OPINION | 80°

This story is part of NSA PHONE TRACKING

Protection for Snowden Russia's latest affront to U.S.

Snowden remains stuck at Moscow airport

Putin warns Snowden not to hurt U.S.-Russian relations

24411

2988

113

3 NSA veterans speak out on whistle-blower: We told you so

Three former NSA whistle-blowers discuss the Edward Snowden case with USA TODAY reporters Susan Page and Peter Eisler.

THAT THE COURTS AND CONGRESS ARE AFFORDED AN OPPORTUNITY TO ENGAGE IN MORE AGGRESSIVE AND BADLY NEEDED OVERSIGHT.

http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/
http://www.dailykos.com/story/2013/06/28/1219618/-Under-Obama-NSA-Continues-Bush-Era-Datamining-on-Americans
http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

http://www.salon.com/2013/06/15/half_of_the_senate_skipped_this_weeks_classified_nsa_briefing/

THE NSA'S UTAH DATACENTER


SECURITY AGENCY
NATIONAL
UNITED STATES OF AMERICA

View the NSA Utah Data Center on Google Maps

View the NSA Utah Data Center on Bing Maps

[FROM FOI REQUESTS] AT NSA'S UTAH DATA CENTER RIBBON CUTTING, AN EMPHASIS ON PRIVATE PARTNERSHIPS AND CLAIMED THAT IT WOULD BE "100% COMMITTED TO PROTECTING THE CIVIL LIBERTIES AND PRIVACY RIGHTS OF THE AMERICAN PEOPLE" [...] "STRENGTHEN AND PROTECT THE NATION'S CYBER-SECURITY." THAT'S A CRITICAL MISSION, ACCORDING TO NSA DIRECTOR GENERAL KEITH ALEXANDER.

DELIVERED MONTHS BEFORE RECENT LEAKS BY FORMER NSA CONTRACTOR EDWARD SNOWDEN SHOWED A POWERPOINT DOCUMENT DETAILING AN NSA PROGRAM, DUBBED PRISM, THAT COLLECTED, ANALYZED AND STORED DATA FROM A NUMBER OF PRIVATE INTERNET COMPANIES.

https://www.muckrock.com/news/archives/2013/jul/11/nsas-utah-data-center-ribbon-cutting-emphasis-priv/

"IT WILL NEED AN AVERAGE OF 65 MEGAWATTS OF ELECTRICITY TO RUN WHAT SEVERAL NSA EQUIPMENT SUPPLIERS SAY WILL BE AMONG THE MOST SOPHISTICATED SUPERCOMPUTERS AND LARGEST RESERVES OF DATA STORAGE ON THE PLANET."

THIS TOP-SECRET DATA WAREHOUSE COULD HOLD AS MANY AS 1.25 MILLION 4-TERABYTE HARD DRIVES, BUILT INTO SOME 5,000 SERVERS TO STORE THE TRILLIONS UPON TRILLIONS OF ONES AND ZEROES THAT MAKE UP YOUR DIGITAL FINGERPRINT. SOME REPORTS HAVE SUGGESTED THE DATA CENTER COULD HOLD AS MUCH AS 5 ZETABYTES.

https://www.muckrock.com/news/archives/2013/jul/11/nsas-utah-data-center-ribbon-cutting-emphasis-priv/

5 Zettabytes (ZB)

=

5,000,000,000,000 Gigabytes (GB)

https://www.muckrock.com/news/archives/2013/jul/11/nsas-utah-data-center-ribbon-cutting-emphasis-priv/

CRAY XC30

Scaling Across the Supercomputer Performance Spectrum

The Cray® XC30™ supercomputer series is the culmination of a powerful industry collaboration and cutting edge HPC research and development. Unlike clusters and "assembled" HPC systems of mixed components requiring user integration, the Cray XC30 series has been specifically designed from the ground up with a holistic approach to optimize the entire system to deliver sustained real-world performance and scalability across all hardware and software. Furthermore, the Cray XC30 series leverages the combined advantages of next-generation Aries™ interconnect and Dragonfly network topology, Intel® Xeon® processors, integrated storage solutions, and major enhancements to the Cray OS and programming environment. The Cray® XC30™ supercomputer is a ground breaking architecture upgradable to 100 Petaflops per system.

DEVELOPMENT OF THE XC30 SERIES WAS FINANCED IN PART BY THE US DEPARTMENT OF DEFENSE (DARPA) TO MEET THE DEMANDING NEEDS OF THE INTELLIGENCE COMMUNITY. SPEEDS ARE UP TO 100 PETAFLOPS, ONE THOUSAND TRILLION CALCULATIONS PER SECOND, OR THREE TIMES FASTER THAN THE WORLD'S CURRENTLY FASTEST COMPUTERS. THIS IS ENOUGH COMPUTER POWER TO TRACK THE MOVEMENTS OF EVERY HUMAN ON EARTH IN REAL TIME AND ALSO ENOUGH TO BREAK ADVANCED ENCRYPTION ALGORITHMS, ACCORDING TO NSA WHISTLEBLOWER WILLIAM BINNEY.

https://secure.flickr.com/photos/villoks/492857088/sizes/l/in/photostream |

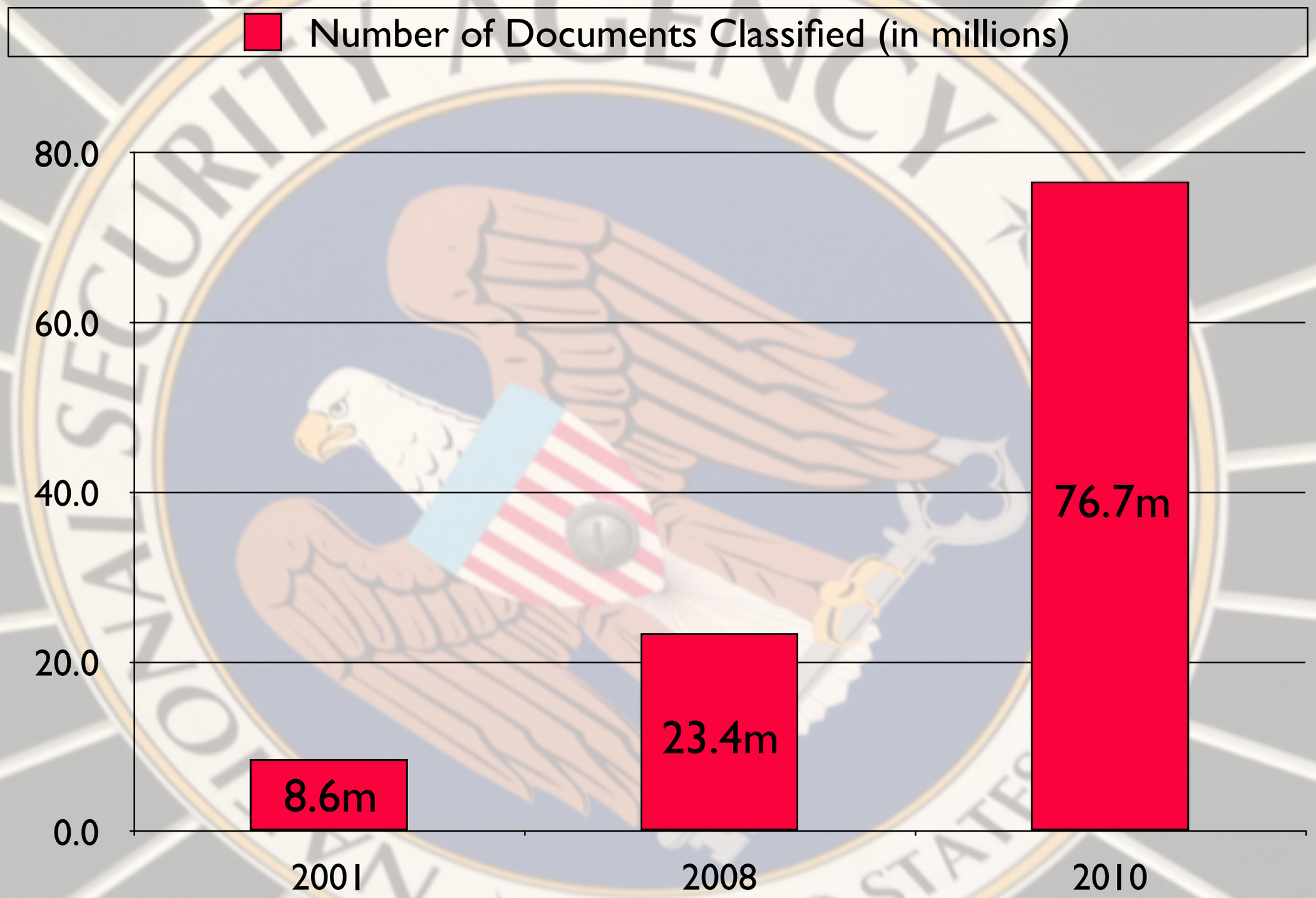
WE CAN MAKE INFERENCES ABOUT THE NSA'S UTAH FACILITY BASED ON THE THEORETICAL AMOUNT OF DATA FROM VARIOUS SOURCES, THE COST OF COMPUTATION, AND THE POWER REQUIREMENTS FROM THE FACILITY, BUT THOSE ARE ROUGH GUESSES AT BEST. FOR A LOT OF THIS, WE'RE COMPLETELY IN THE DARK.[...] THE U.S. GOVERNMENT IS ON A SECRECY BINGE. (AS) IT OVERCLASSIFIES MORE INFORMATION THAN EVER.

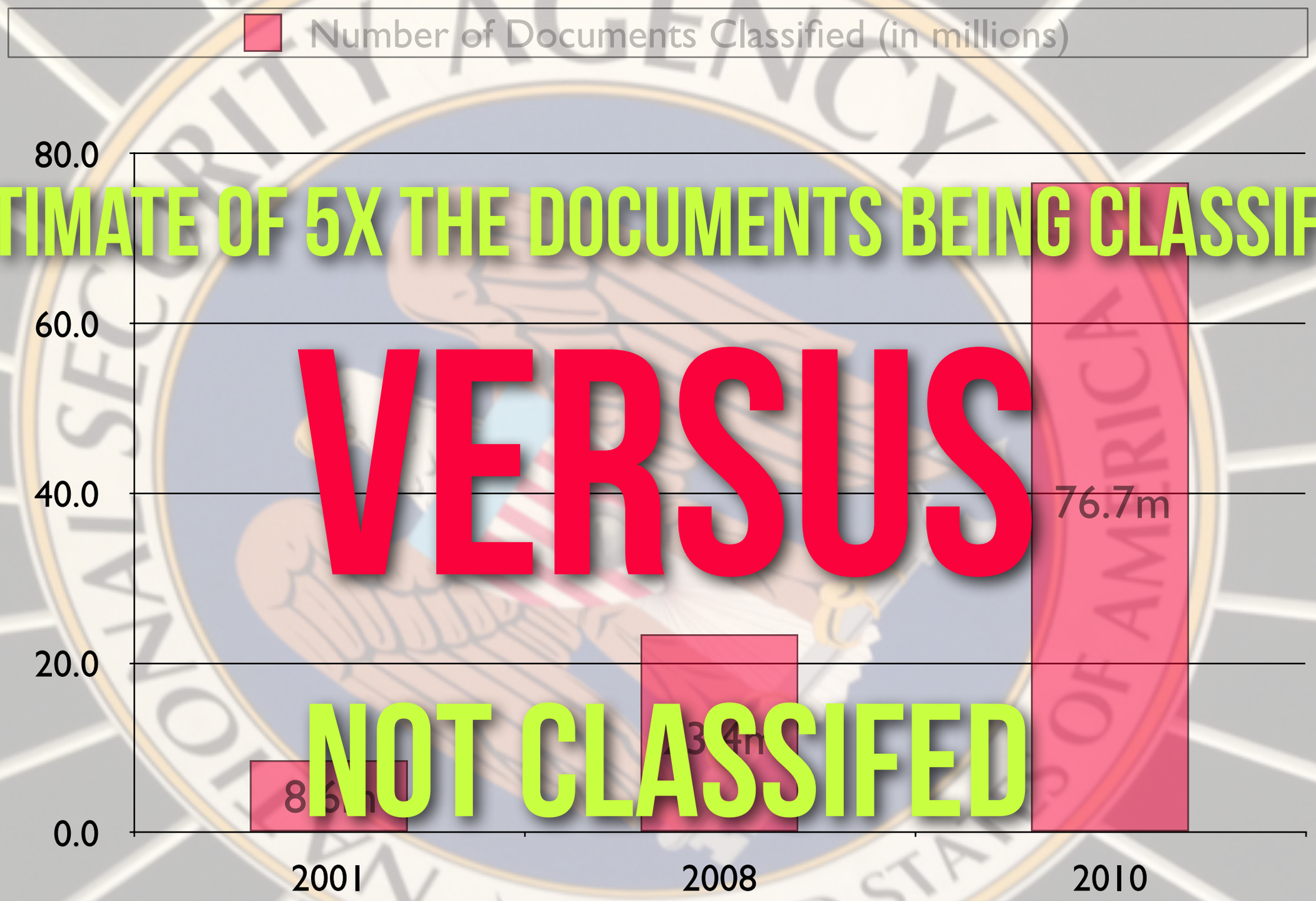
AND WE LEARN, AGAIN AND AGAIN, THAT OUR GOVERNMENT REGULARLY CLASSIFIES THINGS NOT BECAUSE THEY NEED TO BE SECRET, BUT BECAUSE THEIR RELEASE WOULD BE EMBARRASSING.

OUR GOVERNMENT IS PUTTING ITS OWN SELF-INTEREST AHEAD OF THE INTERESTS OF THE COUNTRY. THAT NEEDS TO CHANGE.

BRUCE SCHNEIER

https://www.schneier.com/blog/archives/2013/07/nsa_e-mail_eave.html


Number of Documents Classified (in millions)
80.0
60.0
40.0
20.0
0.0
8.6m
23.4m
76.7m
2001
2008
2010



ESTIMATE OF 5X THE DOCUMENTS BEING CLASSIFIED

VERSUS

NOT CLASSIFED

WE CAN MAKE INFERENCES ABOUT THE NSA'S UTAH FACILITY BASED ON THE THEORETICAL AMOUNT OF DATA FROM VARIOUS SOURCES, THE COST OF COMPUTATION, AND THE POWER REQUIREMENTS FROM THE FACILITY, BUT THOSE ARE ROUGH GUESSES AT BEST. FOR A LOT OF THIS, WE'RE COMPLETELY IN THE DARK.[...] THE U.S. GOVERNMENT IS ON A SECRECY BINGE. (AS) IT OVERCLASSIFIES MORE INFORMATION THAN EVER.

AND WE LEARN, AGAIN AND AGAIN, THAT OUR GOVERNMENT REGULARLY CLASSIFIES THINGS NOT BECAUSE THEY NEED TO BE SECRET, BUT BECAUSE THEIR RELEASE WOULD BE EMBARRASSING.

OUR GOVERNMENT IS PUTTING ITS OWN SELF-INTEREST AHEAD OF THE INTERESTS OF THE COUNTRY. THAT NEEDS TO CHANGE.

BRUCE SCHNEIER

https://www.schneier.com/blog/archives/2013/07/nsa_e-mail_eave.html

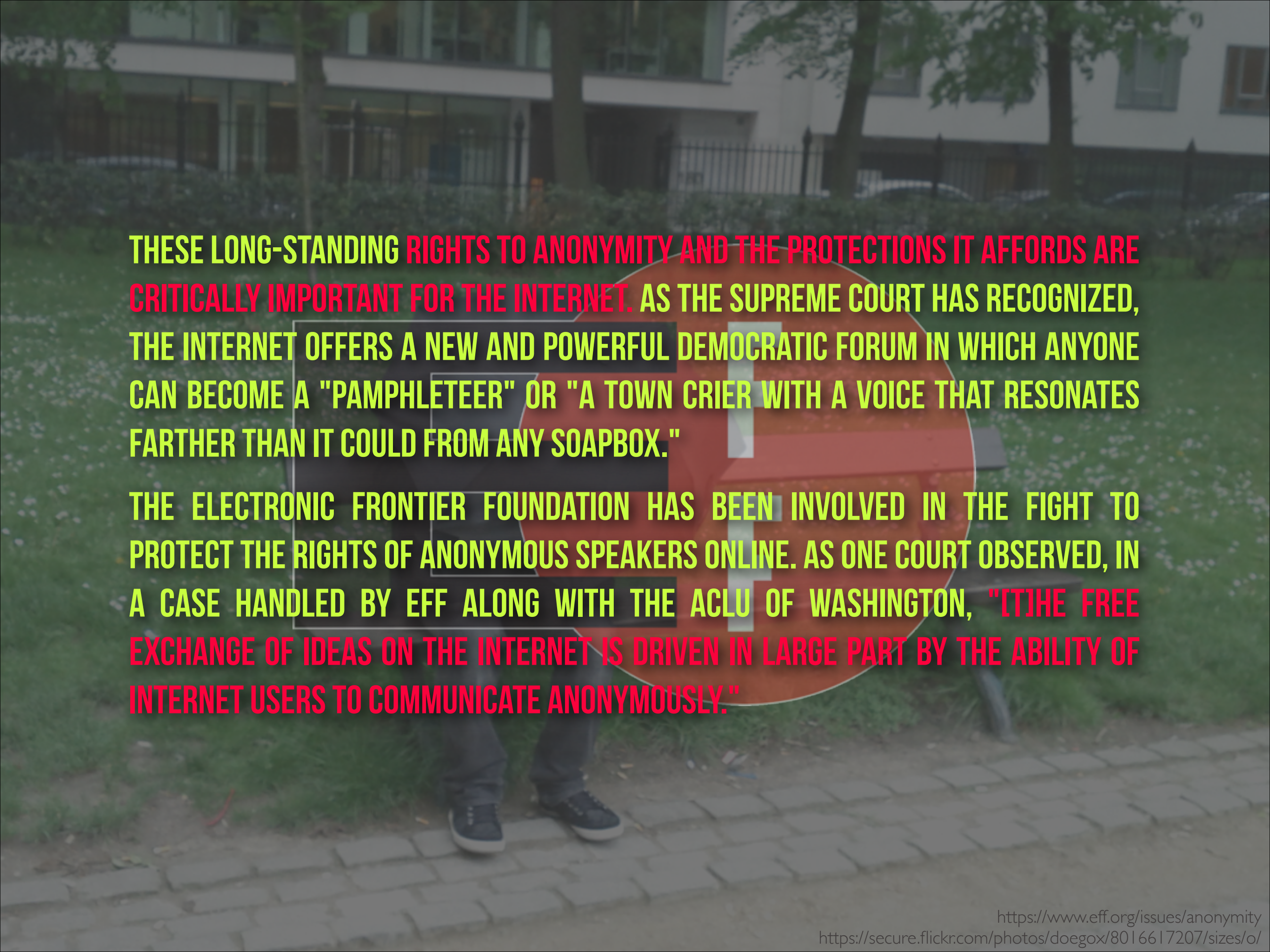

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

PRIVACY AND ANONYMITY IS A RIGHT


https://secure.flickr.com/photos/28096801@N05/4727775848/sizes/l

https://secure.flickr.com/photos/doegox/8016617207/sizes/o/

https://eff.org
https://secure.flickr.com/photos/doegox/8016617207/sizes/o/



THESE LONG-STANDING RIGHTS TO ANONYMITY AND THE PROTECTIONS IT AFFORDS ARE CRITICALLY IMPORTANT FOR THE INTERNET. AS THE SUPREME COURT HAS RECOGNIZED, THE INTERNET OFFERS A NEW AND POWERFUL DEMOCRATIC FORUM IN WHICH ANYONE CAN BECOME A "PAMPHLETEER" OR "A TOWN CRIER WITH A VOICE THAT RESONATES FARTHER THAN IT COULD FROM ANY SOAPBOX."

THE ELECTRONIC FRONTIER FOUNDATION HAS BEEN INVOLVED IN THE FIGHT TO PROTECT THE RIGHTS OF ANONYMOUS SPEAKERS ONLINE. AS ONE COURT OBSERVED, IN A CASE HANDLED BY EFF ALONG WITH THE ACLU OF WASHINGTON, "[T]HE FREE EXCHANGE OF IDEAS ON THE INTERNET IS DRIVEN IN LARGE PART BY THE ABILITY OF INTERNET USERS TO COMMUNICATE ANONYMOUSLY."

https://www.eff.org/issues/anonymity
https://secure.flickr.com/photos/doegox/8016617207/sizes/o/

ANONYMOUS COMMUNICATIONS HAVE AN IMPORTANT PLACE IN OUR POLITICAL AND SOCIAL DISCOURSE. THE SUPREME COURT HAS RULED REPEATEDLY THAT THE RIGHT TO ANONYMOUS FREE SPEECH IS PROTECTED BY THE FIRST AMENDMENT. A MUCH-CITED 1995 SUPREME COURT RULING IN MCINTYRE V. OHIO ELECTIONS COMMISSION READS:

PROTECTIONS FOR ANONYMOUS SPEECH ARE VITAL TO DEMOCRATIC DISCOURSE. ALLOWING DISSENTERS TO SHIELD THEIR IDENTITIES FREES THEM TO EXPRESS CRITICAL MINORITY VIEWS . . . ANONYMITY IS A SHIELD FROM THE TYRANNY OF THE MAJORITY. . . . IT THUS EXEMPLIFIES THE PURPOSE BEHIND THE BILL OF RIGHTS AND OF THE FIRST AMENDMENT IN PARTICULAR: TO PROTECT UNPOPULAR INDIVIDUALS FROM RETALIATION . . . AT THE HAND OF AN INTOLERANT SOCIETY.

https://www.eff.org/issues/anonymity
https://secure.flickr.com/photos/doegox/8016617207/sizes/o/

https://secure.flickr.com/photos/doegox/8016617207/sizes/o/

EMAIL PRIVACY TOOLS/SOFTWARE

https://secure.flickr.com/photos/pagedooley/374202387 1/sizes/l/

Lavabit

My Fellow Users,

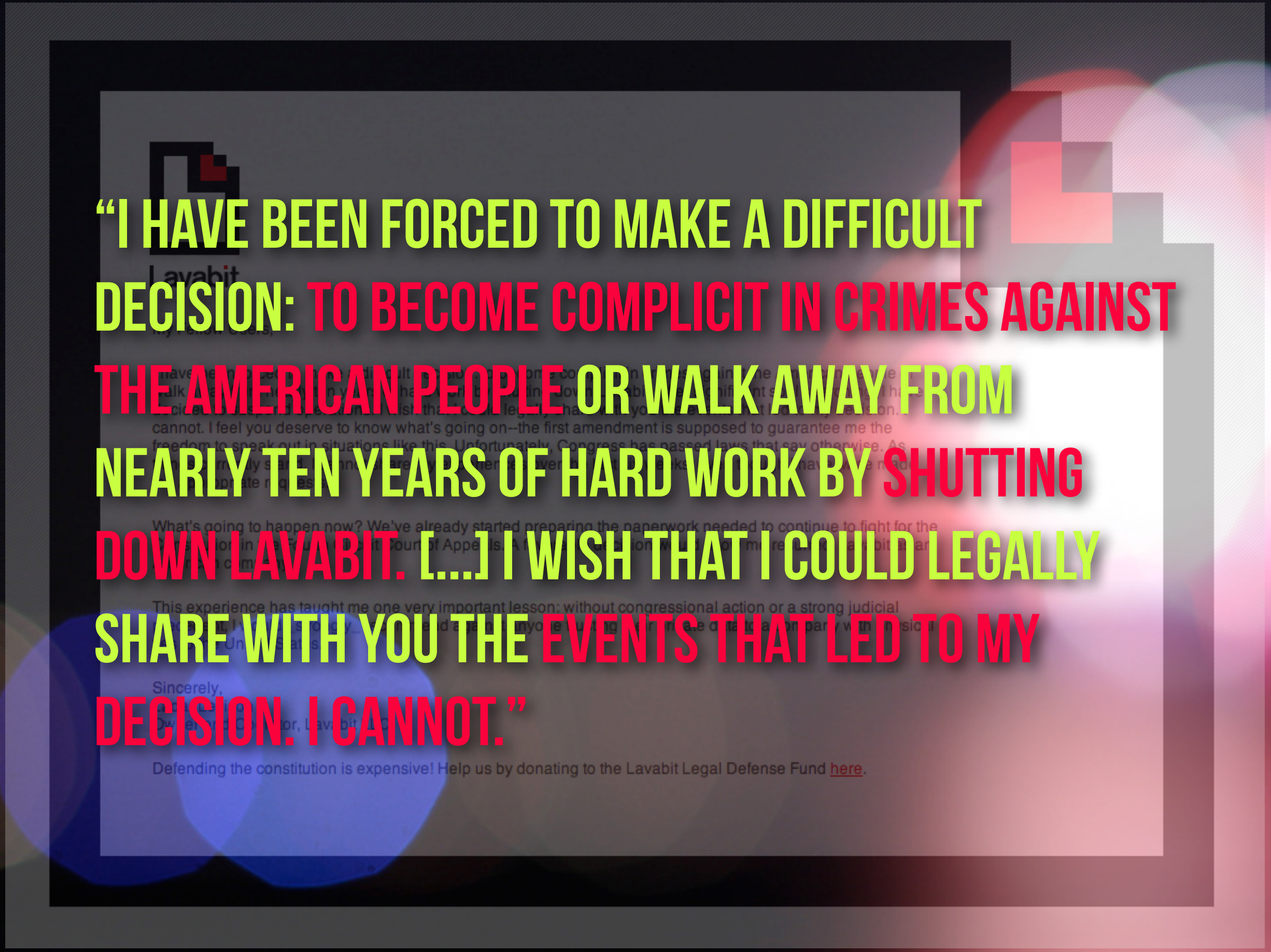
I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

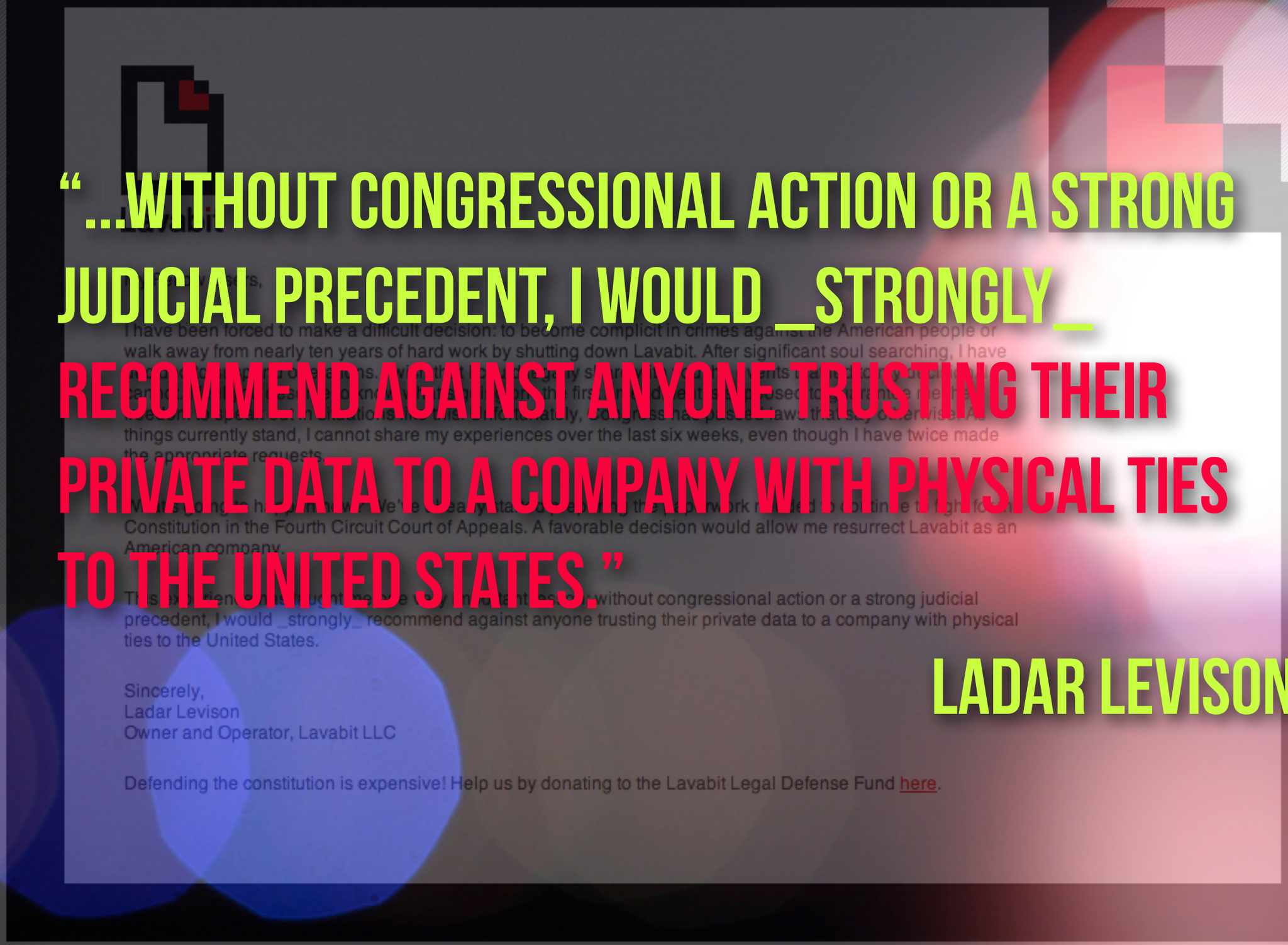
Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.



“I HAVE BEEN FORCED TO MAKE A DIFFICULT DECISION: TO BECOME COMPLICIT IN CRIMES AGAINST THE AMERICAN PEOPLE OR WALK AWAY FROM NEARLY TEN YEARS OF HARD WORK BY SHUTTING DOWN LAVABIT. [...] I WISH THAT I COULD LEGALLY SHARE WITH YOU THE EVENTS THAT LED TO MY DECISION. I CANNOT.”

https://secure.flickr.com/photos/pagedooley/374202387 l/sizes/l/



"...WITHOUT CONGRESSIONAL ACTION OR A STRONG JUDICIAL PRECEDENT, I WOULD _STRONGLY_ RECOMMEND AGAINST ANYONE TRUSTING THEIR PRIVATE DATA TO A COMPANY WITH PHYSICAL TIES TO THE UNITED STATES."

LADAR LEVISON

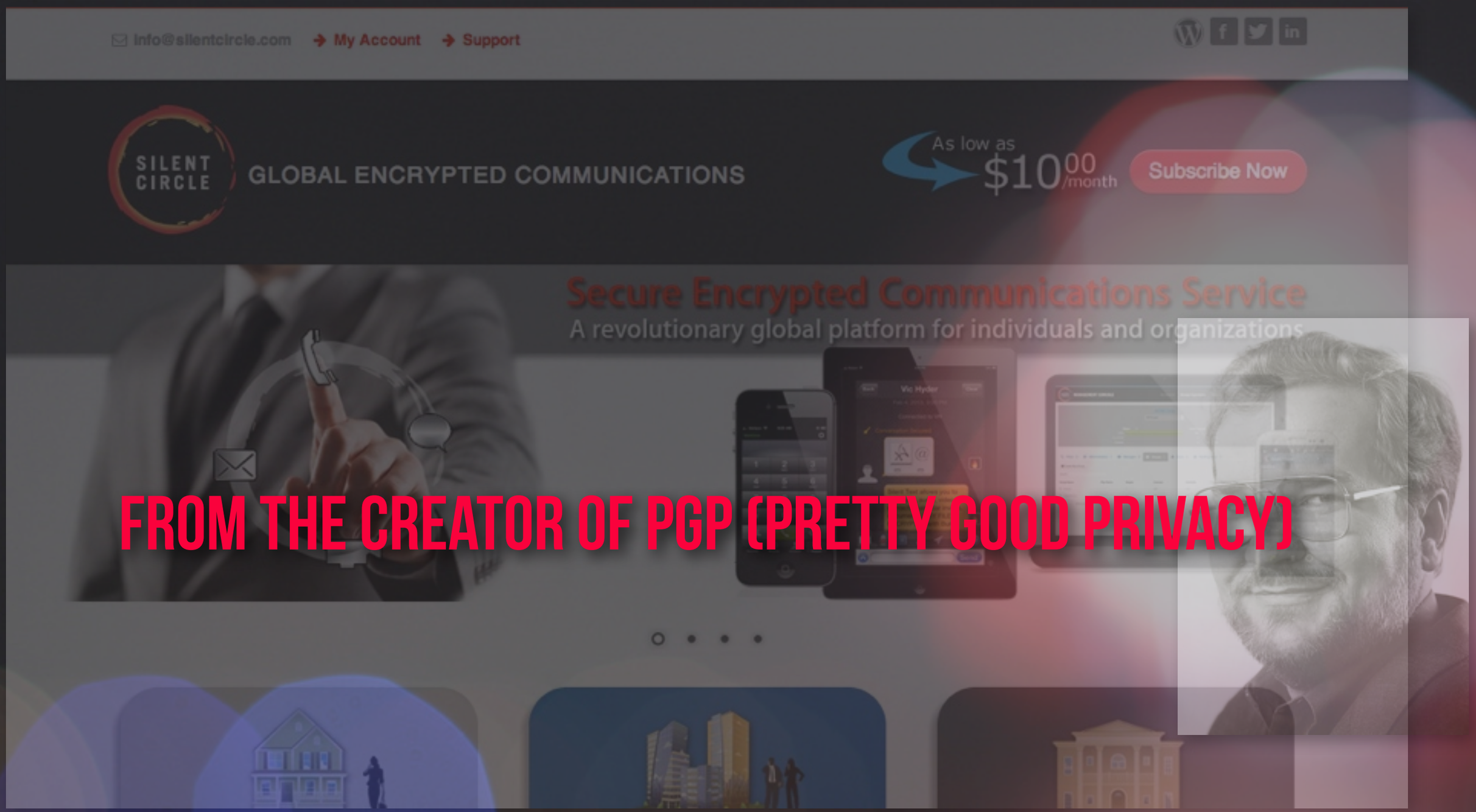
https://secure.flickr.com/photos/pagedooley/374202387 l/sizes/l/

GLOBAL ENCRYPTED COMMUNICATIONS

https://silentcircle.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

GLOBAL ENCRYPTED COMMUNICATIONS

https://en.wikipedia.org/wiki/File:PRZ_closeup_cropped.jpg
https://silentcircle.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

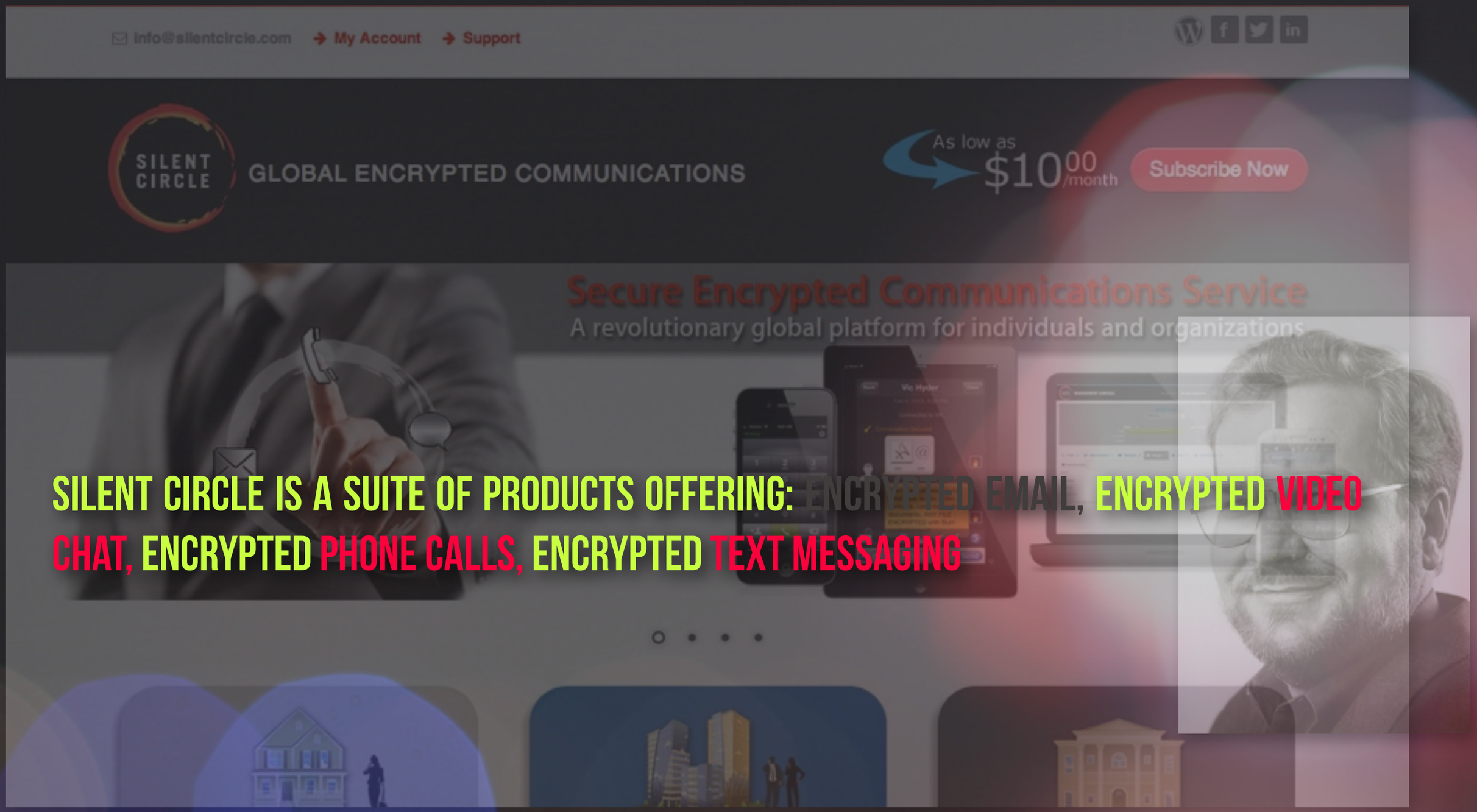


GLOBAL ENCRYPTED COMMUNICATIONS

https://en.wikipedia.org/wiki/File:PRZ_closeup_cropped.jpg
https://silentcircle.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

GLOBAL ENCRYPTED COMMUNICATIONS

https://en.wikipedia.org/wiki/File:PRZ_closeup_cropped.jpg
https://silentcircle.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/



GLOBAL ENCRYPTED COMMUNICATIONS

https://en.wikipedia.org/wiki/File:PRZ_closeup_cropped.jpg
https://silentcircle.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

start.mail

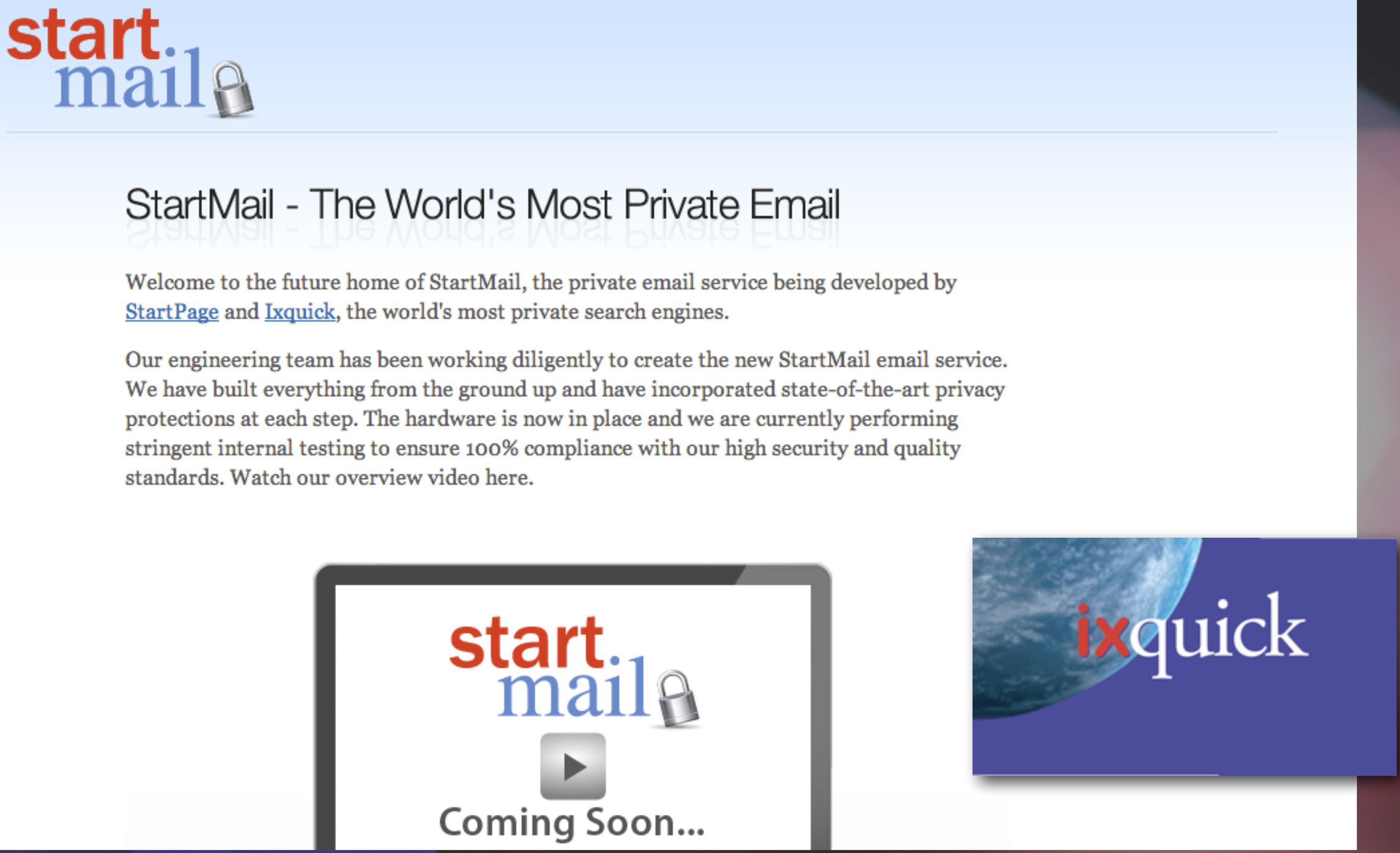
StartMail - The World's Most Private Email

Welcome to the future home of StartMail, the private email service being developed by StartPage and Ixquick, the world's most private search engines.

Our engineering team has been working diligently to create the new StartMail email service. We have built everything from the ground up and have incorporated state-of-the-art privacy protections at each step. The hardware is now in place and we are currently performing stringent internal testing to ensure 100% compliance with our high security and quality standards. Watch our overview video here.

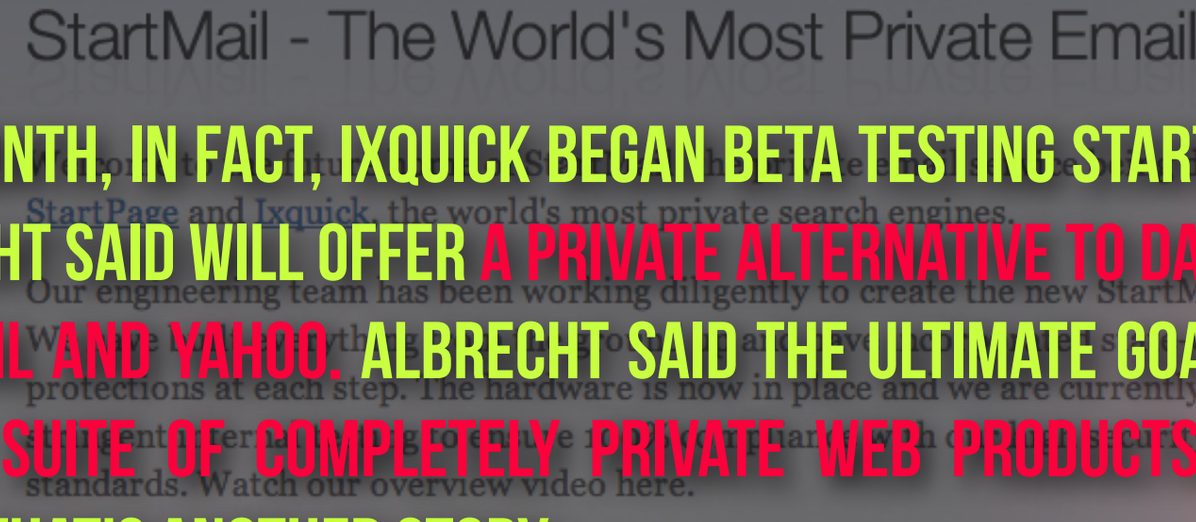
"WORLD'S MOST PRIVATE EMAIL"

https://startmail.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/



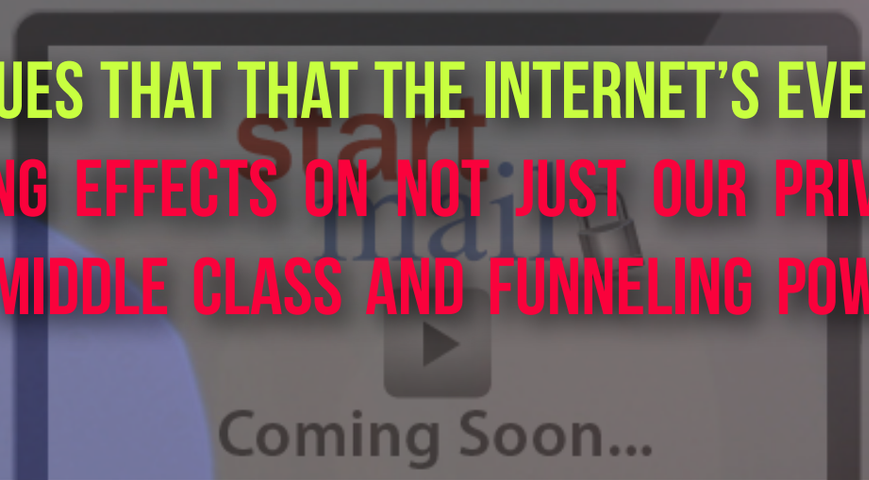
"WORLD'S MOST PRIVATE EMAIL"

https://startmail.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/



THIS MONTH, IN FACT, IXQUICK BEGAN BETA TESTING STARTMAIL, AN EMAIL SERVICE THAT ALBRECHT SAID WILL OFFER A PRIVATE ALTERNATIVE TO DATA-COLLECTING SERVICES SUCH AS GMAIL AND YAHOO. ALBRECHT SAID THE ULTIMATE GOAL FOR IXQUICK IS TO OFFER AN ENTIRE SUITE OF COMPLETELY PRIVATE WEB PRODUCTS. CONVINCING PEOPLE TO USE THEM? THAT'S ANOTHER STORY.

... JARON LANIER ARGUES THAT THAT THE INTERNET'S EVER-GROWING "CULTURE OF FREE" HAS HAD DEVASTATING EFFECTS ON NOT JUST OUR PRIVACY BUT ALSO OUR ECONOMY, DISSEMINATING THE MIDDLE CLASS AND FUNNELING POWER INTO A FEW MONOPOLISTIC COMPANIES.



"WORLD'S MOST PRIVATE EMAIL"

http://www.ibtimes.com/alternatives-google-gmail-private-search-email-services-promise-online-anonymity-wake-nsa-1317983
https://startmail.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

StartMail - The World's Most Private Email

Welcome to the future home of StartMail, the private email service being developed by StartPage and Ixquick, the world's most private search engines.

Our engineering team has been working diligently to create the new StartMail email service. We have built everything from the ground up and have incorporated state-of-the-art privacy protections at each step. The hardware is now in place and we are currently performing
standards. Watch our overview video here.

THE QUESTION, THEN, BECOMES WHETHER OR NOT CONSUMERS WILL EVER WRAP THEIR HEADS AROUND THE IDEA OF PAYING FOR EMAIL. ALBRECHT ACKNOWLEDGES THE CHALLENGE, BUT SHE SAID IT'S ULTIMATELY A MATTER OF PAYING WITH YOUR WALLET OR WITH YOUR DATA.

"WORLD'S MOST PRIVATE EMAIL"

http://www.ibtimes.com/alternatives-google-gmail-private-search-email-services-promise-online-anonymity-wake-nsa-1317983
https://startmail.com/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

NSA-PROOF MESSENGER APP

http://bestseedbox.net/2013/07/10/pirate-bay-founder-to-launch-nsa-proof-messenger-app/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

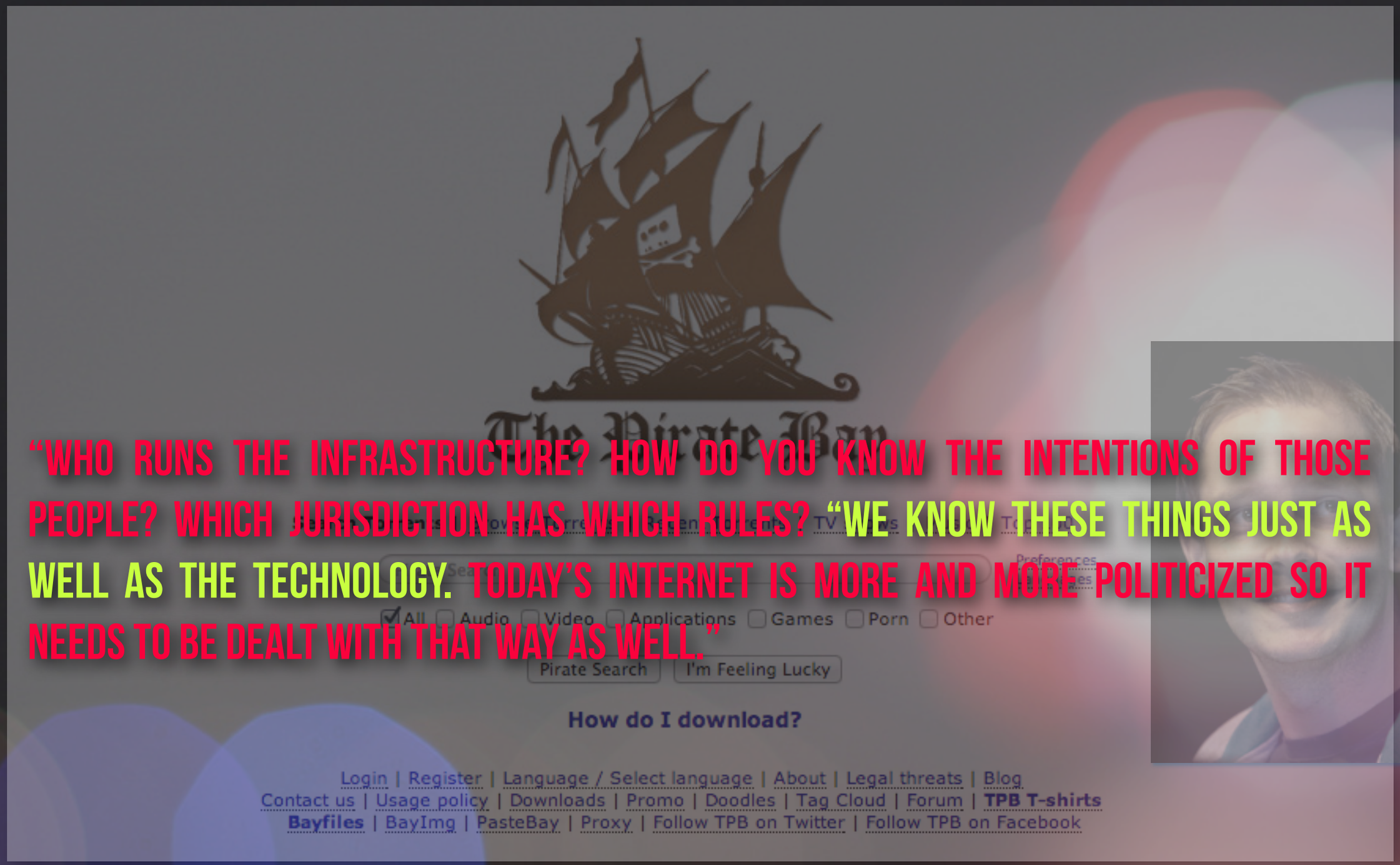
NSA-PROOF MESSENGER APP

http://bestseedbox.net/2013/07/10/pirate-bay-founder-to-launch-nsa-proof-messenger-app/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

"IN THIS DAY AND AGE WE CAN'T DO WITHOUT ENCRYPTION"

NSA-PROOF MESSENGER APP

http://bestseedbox.net/2013/07/10/pirate-bay-founder-to-launch-nsa-proof-messenger-app/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/



"WHO RUNS THE INFRASTRUCTURE? HOW DO YOU KNOW THE INTENTIONS OF THOSE PEOPLE? WHICH JURISDICTION HAS WHICH RULES? "WE KNOW THESE THINGS JUST AS WELL AS THE TECHNOLOGY. TODAY'S INTERNET IS MORE AND MORE POLITICIZED SO IT NEEDS TO BE DEALT WITH THAT WAY AS WELL."

NSA-PROOF MESSENGER APP

http://bestseedbox.net/2013/07/10/pirate-bay-founder-to-launch-nsa-proof-messenger-app/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

Dotcom's Mega Debuts Spy-Proof Messaging This Summer, Email Follows

Ernesto

July 11, 2013

136

encryption, privact

Print

Catering to the demands of millions of people, Kim Dotcom's Mega is planning to release its encrypted messaging service in four to six weeks. The company will first roll out a web-based messaging platform, soon to be followed by apps and encrypted email. According to Mega CEO Vikram Kumar the Internet is the battleground of a new crypto war, which will not be lost by the public.

The NSA PRISM scandal and the global increase in online surveillance has increased the demand for more private means of communications.

The traceless search engine DuckDuckGo has witnessed a massive boost in visitors, and this week the new encrypted messaging service from Peter Sunde raised $100,000 via crowd-funding in just one day.

Kim Dotcom's Mega, which brands itself as "The Privacy Company," is also expanding its offering in the encryption niche. Currently the site allows users to store their files fully

NewsBits

Even more news...

TV Station Covers Up "Ho Lee Fuk" Blunder With a DMCA Takedown

By now most people have probably seen KTVU's embarrassing blunder, reading the made-up names of Asiana...

Prenda Loses Again, Hit for $22,000

The continuing Prenda Law debacle has just resulted in another defeat for the world's most famous...

Clueless Law Enforcement Try to Track Down IP Address Users

Among the responsibilities of the non-profit RIPE NCC organization is to hand out IP addresses in...

EFF Sues U.S. Government to Stop NSA Spying

The Electronic Frontier Foundation has filed a lawsuit against the NSA's spy programs. The EFF is...

Police Investigate Dotcom's Face Projected Onto U.S. Embassy

Last weekend the words "United Stasi of America" were projected onto the side of the US...

SPY-PROOF MESSENGING

https://torrentfreak.com/dotcoms-mega-debuts-spy-proof-messaging-this-summer-email-follows-130711/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

TorrentFreak

Home About Archives Categories News Bits Contact

The place where breaking news, BitTorrent and copyright collide

Subscribe via RSS Subscribe via Email Tip Us Off!

Search TorrentFreak

Type Search Term Here... Search

Dotcom's Mega Debuts Spy-Proof Messaging This Summer, Email Follows

Ernesto

July 11, 2013

136

encryption, privact

Print

Catering to the demands of millions of people, Kim Dotcom's Mega is planning to release its encrypted messaging service in four to six weeks. The company will first roll out a web-based messaging platform, soon to be followed by apps and encrypted email. According to Mega CEO Vikram Kumar the Internet is the battleground of a new crypto war, which will not be lost by the public.

The NSA PRISM scandal and the global increase in online surveillance has increased the demand for more private means of communications.

MEGA BETA

The traceless search engine DuckDuckGo has witnessed a massive boost in visitors, and this week the new encrypted messaging service from Peter Sunde raised $100,000 via crowd-funding in just one day.

Kim Dotcom's Mega, which brands itself as "The Privacy Company," is also expanding its offering in the encryption niche. Currently the site allows users to store their files fully

NewsBits

Even more news...

TV Station Covers a DMCA Takedow

By now most people embarrassing blunde Asiana...

Prenda Loses Aga

The continuing Prenc another defeat for the

Clueless Law Enfo Address Users

Among the responsib organization is to har

EFF Sues U.S. Gov

The Electronic Fronti against the NSA's sp

Police Investigate U.S. Embassy

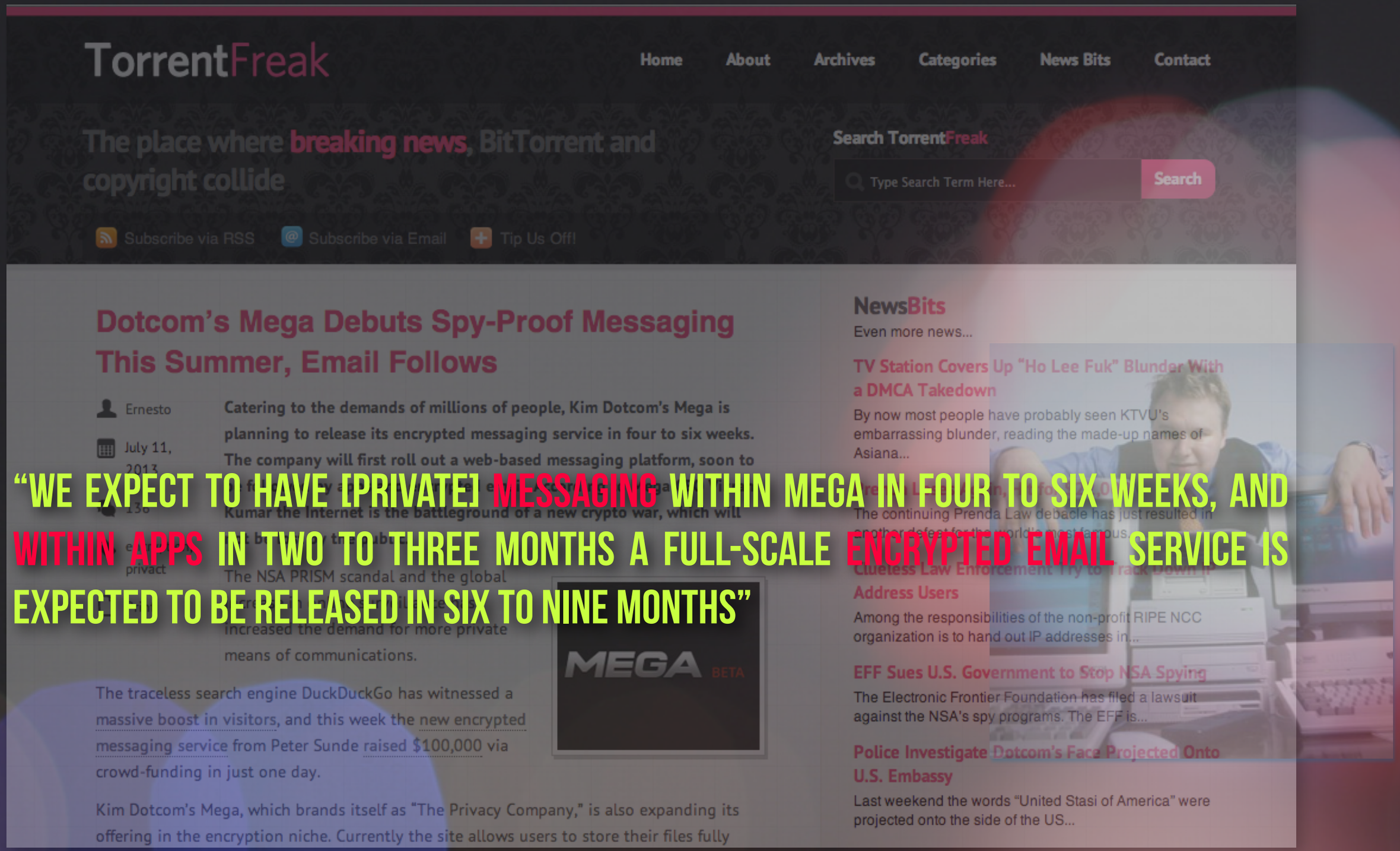
Last weekend the words "United Stasi of America" were projected onto the side of the US...

SPY-PROOF MESSENGING

https://en.wikipedia.org/wiki/Kim_dotcom

https://torrentfreak.com/dotcoms-mega-debuts-spy-proof-messaging-this-summer-email-follows-130711/

https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/



"WE EXPECT TO HAVE [PRIVATE] MESSAGING WITHIN MEGA IN FOUR TO SIX WEEKS, AND WITHIN APPS IN TWO TO THREE MONTHS A FULL-SCALE ENCRYPTED EMAIL SERVICE IS EXPECTED TO BE RELEASED IN SIX TO NINE MONTHS"

SPY-PROOF MESSENGING

https://en.wikipedia.org/wiki/Kim_dotcom
https://torrentfreak.com/dotcoms-mega-debuts-spy-proof-messaging-this-summer-email-follows-130711/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

PURPOSE BUILT PRIVACY TOOLS

http://www.newyorker.com/strongbox/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

STRONGBOX IS [...] DESIGNED TO PROVIDE YOU WITH A GREATER DEGREE OF ANONYMITY AND SECURITY THAN AFFORDED BY CONVENTIONAL E-MAIL.

TO HELP PROTECT YOUR ANONYMITY, STRONGBOX IS ONLY ACCESSIBLE USING THE TOR NETWORK. WHEN USING STRONGBOX, THE NEW YORKER WILL NOT RECORD YOUR I.P. ADDRESS OR INFORMATION ABOUT YOUR BROWSER, COMPUTER, OR OPERATING SYSTEM, NOR WILL WE EMBED THIRD-PARTY CONTENT OR DELIVER COOKIES TO YOUR BROWSER.

PURPOSE BUILT PRIVACY TOOLS

http://www.newyorker.com/strongbox/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

DeadDrop

Fork DeadDrop
DeadDrop Documentation

DeadDrop is a server application intended to let news organizations and others set up an online drop box for sources. It's open source software written by Aaron Swartz in consultation with a volunteer team of security experts. In addition to Aaron's code, the project includes installation scripts and set-up instructions both for the software, and for a hardened Ubuntu environment on which to run it.

DeadDrop was created with the goal of placing a secure drop box within reach of anyone with the need. But at this point expertise is still required to safety deploy this software. And the software itself needs more work.

DeadDrop is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version. This program, and all material accompanying it, is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU

PURPOSE BUILT PRIVACY TOOLS

http://deaddrop.github.io/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

DeadDrop

Fork DeadDrop
DeadDrop Documentation

DeadDrop is a server application intended to let news organizations and others s
drop box for sources. It's open source software written by Aaron Swartz in consult
volunteer team of security experts. In addition to Aaron's code, the project include
scripts and set-up instructions both for the software, and for a hardened Ubuntu e
which to run it.

DeadDrop was created with the goal of placing a secure drop box within reach of
the need. But at this point expertise is still required to safety deploy this software.
software itself needs more work.

DeadDrop is free software: you can redistribute it and/or modify it under the term
Affero General Public License as published by the Free Software Foundation, eith
the License, or (at your option) any later version. This program, and all material accompanying it,
is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the
implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU

PURPOSE BUILT PRIVACY TOOLS

http://deaddrop.github.io/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

IN OPERATION, EVERY SOURCE IS GIVEN A UNIQUE "CODENAME." THE CODENAME LETS THE SOURCE ESTABLISH A RELATIONSHIP WITH THE NEWS ORGANIZATION WITHOUT REVEALING HER REAL IDENTITY OR RESORTING TO E-MAIL. SHE CAN ENTER THE CODE NAME ON A FUTURE VISIT TO READ ANY MESSAGES SENT BACK FROM THE JOURNALIST

PURPOSE BUILT PRIVACY TOOLS

http://deaddrop.github.io/
https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

https://secure.flickr.com/photos/pagedooley/3742023871/sizes/l/

SHIPPING YOUR EMAIL OFFSHORE

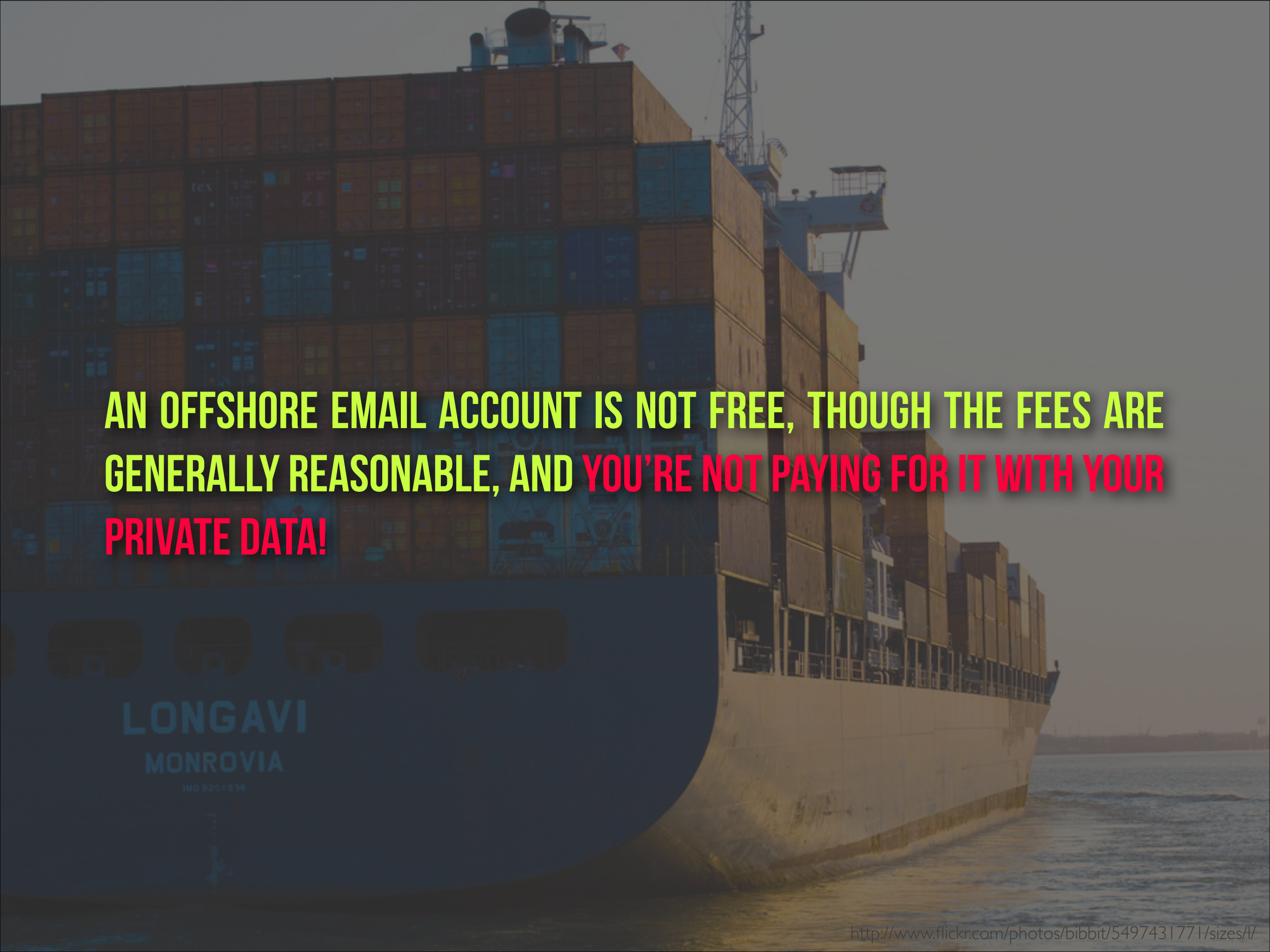
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

WHILE SOME COUNTRIES SEE THEIR EMAIL PRIVACY REGULATIONS ATTACKED OR BREACHED, OFFSHORE EMAIL SERVICES IN EUROPEAN COUNTRIES (ASIA AND ELSEWHERE) CAN GENERALLY OFFER STRONGER EMAIL PRIVACY TO BOTH INDIVIDUALS AND COMPANIES WORLDWIDE.

IN ELECTRONIC COMMUNICATION, THIS PRINCIPLE PROTECTS NOT ONLY THE MESSAGE CONTENTS BUT ALSO THE LOGS OF WHEN AND FROM/TO WHOM MESSAGES HAVE BEEN SENT.

IN NORWAY, FREEDOM OF EXPRESSION AND PRIVACY OF CORRESPONDENCE IS GOVERNED BY THE NORWEGIAN HUMAN RIGHTS ACT, ESPECIALLY ARTICLE 8: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE.

https://secure.runbox.com/why-runbox/email-privacy-offshore-email/
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/



AN OFFSHORE EMAIL ACCOUNT IS NOT FREE, THOUGH THE FEES ARE GENERALLY REASONABLE, AND YOU'RE NOT PAYING FOR IT WITH YOUR PRIVATE DATA!

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

There's no such thing as

free email

Privacy is priceless.

runbox.com™

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

runbox
Premium Email Services

your private secure
MUTEMAIL

Privacy.li
Privacy is your right, but you must defend it

Unspyable
Offshore Email & Personal VPN Service - Secure your Internet

TheAnonymousEmail.com
Anonymous Internet Services Since 2003

generalmail.com
swissmail.org

shinjiru

NEOMAILBOX

SurfBouncer

TorGuard
Online Privacy Protection Services

KeptPrivate.com

http://www.flickr.com/photos/bibbit/5497431771/sizes//

runbox
Premium Email Services

your private secure
MUTEMAIL

Privacy.li
Privacy is your right, but you must defend it

Unspyable
Offshore Email & Personal VPN Service - Secure your Internet

TheAnonymousEmail.com
Anonymous Internet Services Since 2003

generalmail.com

swissmail.org

shinjiru

NEOMAILBOX

TorGuard
Online Privacy Protection Services

SurfBouncer

LONGAVI
MONROVIA

KEPTPRIVATE.COM

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

PERSONAL DATA MUST ONLY BE COLLECTED BY PRIVATE ENTITIES WHEN CONSENT FROM THE USER HAS BEEN OBTAINED.

PERSONAL DATA MUST NOT BE USED FOR PURPOSES INCONSISTENT WITH THE INITIAL PURPOSE OF COLLECTION EXCEPT WITH CONSENT FROM THE USER.

PERSONAL DATA MUST NOT BE STORED LONGER THAN REQUIRED BY THE PURPOSE OF COLLECTION.

PERSONAL DATA MUST BE KEPT CONFIDENTIAL UNLESS REQUIRED BY LAW.

DO NOT SELL OR PASS ON ANY INFORMATION ABOUT OUR USERS TO ANY THIRD PARTY.

OPENPGP ENCRYPTION, DIGITAL SIGNATURES.

http://www.shinjiru.com/web_hosting/email_hosting/private-email-hosting.php
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

SHINJIRU IS **HUSHMAIL'S OFFICIAL PARTNER** & RESELLER IN MALAYSIA.

HUSHTOOLS, OUR **ENCRYPTION TOOLKIT,** USES USING OPEN PGP (2048 BIT ENCRYPTION) STANDARD ALGORITHMS.

MALAYSIA
SINGAPORE
HOLLAND

MESSAGES [BETWEEN USERS] ARE ENCRYPTED BEFORE LEAVING THE SENDER'S COMPUTER AND REMAIN ENCRYPTED UNTIL AFTER THEY ARRIVE ON THE RECIPIENT'S.

DIGITAL SIGNATURES FOR EMAIL AND ATTACHMENTS, END-TO-END ENCRYPTION FOR EMAIL AND FILES.

HUSH MESSENGER FOR SECURE INSTANT MESSAGING.

IP ADDRESS IS REMOVED FROM ALL OUTGOING EMAILS.

http://www.shinjiru.com/web_hosting/email_hosting/private-email-hosting.php
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

http://mutemail.com//
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

SERVERS ARE OFFSHORE IN BAHAMAS, A COUNTRY WITH STRICT PRIVACY LAWS.

ALL TRAFFIC IS TRANSFERRED THROUGH AN SSL ENCRYPTED CONNECTION BETWEEN CUSTOMER'S EMAIL SOFTWARE AND OUR SECURE EMAIL SERVERS.

ADDITIONAL NON-STANDARD SMTP PORT FOR CLIENTS, WHICH MAY BE OF USE IF CLIENT'S ISP OR COMPANY FIREWALL BLOCKS REMOTE EMAIL ACCOUNT ACCESS.

BAHAMAS

IP ADDRESS AND HOST NAME IS NOT SHOWN IN THE MESSAGE HEADERS.

THEY DO NOT KEEP THESE ANY RECORDS OF IP ADDRESSES ASSOCIATED WITH ANY RECEIVED EMAILS.

THEY DO NOT LOG ANYTHING.

http://mutemail.com//
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

http://www.trilightzone.org/secureemail.html
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

SERVER SYSTEMS ARE COMPLETELY REALTIME ENCRYPTED INCLUDING YOUR EMAIL.

YOUR IP IS NEVER VISIBLE

WEBMAIL HAS PGP SUPPORT WITH UP TO 4096 BITS KEYS.

NO LOGS KEPT - NO JAVA OR JAVASCRIPT REQUIRED.

NETHERLANDS
LUXEMBOURG
HONG KONG
MALAYSIA

AVAILABLE OFFSHORE SSH PRIVACY TUNNEL & TRISHELL JURISDICTIONS.

PAYMENT OPTIONS: PECUNIX, BITCOIN, PAYPAL, CREDITCARD, CASH, LITECOIN, BANKWIRE, MONEYORDER.

THEY BLOG, POST ARTICLES COVERING ONLINE PRIVACY AND ANONYMITY.

THEY LIST THEIR PUBLIC KEY ON THE SITE.

http://www.trilightzone.org/securemail.html
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

NEOMAILBOX

http://www.neomailbox.com/services/secure-email
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

THEY BELIEVE THAT THIS TRADITIONAL RESPECT FOR PRIVACY, MAKES SWITZERLAND AN IDEAL LOCATION FOR PREMIUM PRIVATE EMAIL HOSTING.

IP ANONYMIZATION, INTERNET ADDRESS AND GEOGRAPHICAL LOCATION IS NOT REVEALED TO RECIPIENTS OF YOUR EMAILS (IP HIDING).

SWITZERLAND ALTERNATE PORTS AVAILABLE FOR USE FROM BEHIND CORPORATE / ISP FIREWALLS.

UNLIMITED DISPOSABLE EMAIL ADDRESSES, VIRUS BLOCKING WITH CLAMAV.

LOGS KEPT FOR 7 DAYS FOR PERFORMANCE ANALYSIS, ABUSE PREVENTION.

ALSO OFFERS ANONYMOUS SURFING, ANONYMOUS SURFING LOGS ARE DELETED EVERY 10 MINUTES.

http://www.neomailbox.com/services/secure-email
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

TWO-FACTOR AUTHENTICATION + OPTIONAL HARDWARE TOKEN.

SECURE OPENBSD SERVERS, THE MOST SECURE OPERATING SYSTEM AVAILABLE, KEPT UP TO DATE WITH THE LATEST SECURITY PATCHES.

SWITZERLAND HARDWARE-ACCELERATED SSL ENCRYPTION PROVIDES FAST ACCESS TO SECURE SERVICES.

DOES NOT REQUEST OR REQUIRE ANY IDENTIFIABLE PERSONAL INFORMATION WHEN YOU CREATE AN ACCOUNT, ALTHOUGH CREDIT CARDS DO REVEAL PERSONAL INFORMATION TO VALIDATE THE PURCHASE.

PAYMENT IN DIGITAL GOLD CURRENCIES FOR INCREASED CUSTOMER PRIVACY - SO YOU DON'T HAVE TO REVEAL ANY PERSONAL DETAILS

http://www.neomailbox.com/services/secure-email
http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

runbox
Premium Email Services

your private secure
MUTEMAIL

Privacy.li
Privacy is your right, but you must defend it

Unspyable
Offshore Email & Personal VPN Service - Secure your Internet

TheAnonymousEmail.com
Anonymous Internet Services Since 2003

generalmail.com
swissmail.org

shinjiru

NEOMAILBOX

SurfBouncer

TorGuard
Online Privacy Protection Services

KeptPrivate.com

http://www.flickr.com/photos/bibbit/5497431771/sizes//

bitcoin

AMERICAN EXPRESS

DWOLLA

WebMoney

litecoin

OKPAY

Payza

PayPal™

MasterCard

pecunix
money refined

VISA

Perfect Money PM
Just perfect

DISCOVER
NETWORK

moneybookers
Skrill

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

bitcoin

AMERICAN EXPRESS

DWOLLA

WebMoney

litecoin

OKPAY

Payza

PayPal

MasterCard

pecunix
money refined

VISA

Perfect Money PM
Just perfect

DISCOVER
NETWORK

moneybookers
Skrill

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

http://www.flickr.com/photos/bibbit/5497431771/sizes/l/

RESOURCES FOR IMPROVEMENT/DIY


https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

Surveillance Self-Defense

Donate to EFF

The SSD Project

- Risk Management
- Data Stored on Your Computer
- Data on the Wire
- Information Stored By Third Parties
- Foreign Intelligence and Terrorism Investigations
- Defensive Technology
  - Internet Basics
  - Encryption Basics
  - Web Browsers
  - **Email**
  - Instant Messaging (IM)
  - Wi-Fi
  - Tor
  - Malware
  - Mobile Devices
  - Secure Deletion
  - File and Disk Encryption
  - Virtual Private Networks (VPN)
  - Voice over Internet Protocol (VoIP)

Search

Questions? Feedback? Contact us.

View a print-friendly version of this site

Email

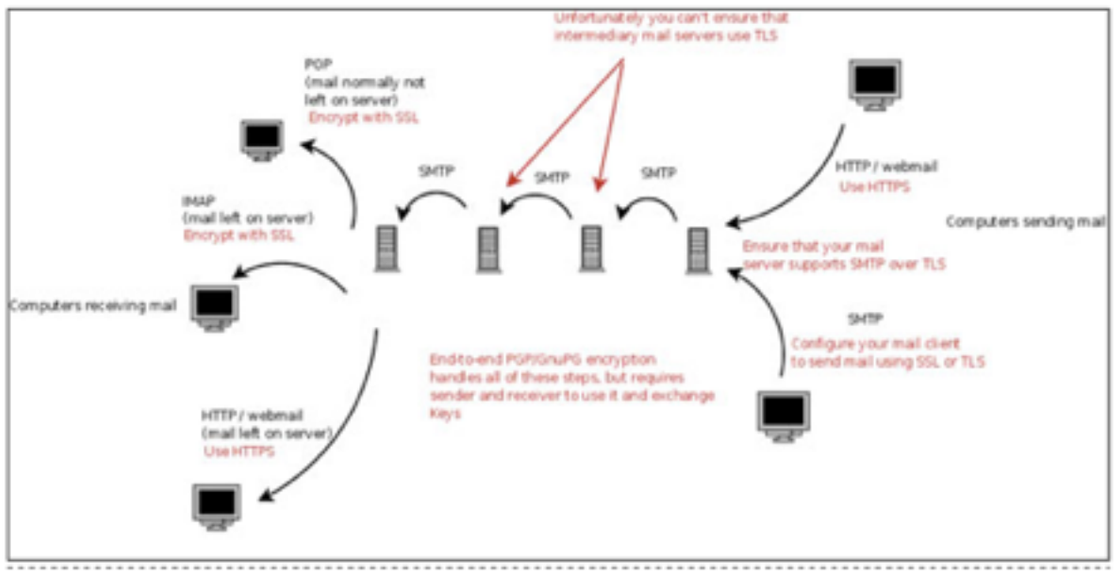
The act of using email stores data on your machines, transmits data over the network, and stores data on third party machines.

Locally Stored Data

The usual measures apply to managing the copies of emails (both sent and received) that are kept on your own machines. Encrypt your drives and decide upon and follow an appropriate data deletion policy.

Data on the Wire

Email usually travels through a number of separate hops between the sender and receiver. This diagram illustrates the typical steps messages might travel through, the transmission protocols used for those steps, and the available types of encryption for those steps.



End-to-End Encryption of Specific Emails

Encrypting emails all the way from the sender to the receiver has historically been difficult, although the tools for achieving this kind of end-to-end encryption are getting better and easier to use. Pretty Good Privacy (PGP) and its free cousin GNU Privacy Guard (GnuPG) are the standard tools for doing this. Both of these programs can provide protection for your email in transit and also protect your stored data. Major email clients such as Microsoft Outlook and Mozilla Thunderbird can be configured to

https://ssd.eff.org/tech/email

https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

FREEDOM
OF THE PRESS
FOUNDATION

Home About Organizations Get Involved Blog Manning Transcripts Digital Security

Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance

July 2, 2013

By Micah Lee

View this whitepaper in PDF form.

> *Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.*
>
> – Edward Snowden, answering questions live on the Guardian's website

The NSA is the biggest, best funded spy agency the world has ever seen. They spend billions upon billions of dollars each year doing everything they can to vacuum up the digital communications of most humans on this planet that have access to the Internet and and the phone network. And as the recent reports in the Guardian and Washington Post show, even domestic American communications are not safe from their net.

Defending yourself against the NSA, or any other government intelligence agency, is not simple, and it's not something that can be solved just by downloading an app. But thanks to the dedicated work of civilian cryptographers and the free and open source software community, it's still possible to have privacy on the Internet, and the software to do it is freely available to everyone. This is especially important for journalists communicating with sources online.

Table of Contents

https://pressfreedomfoundation.org/encryption-works
https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

riseup.net

Home | Email | Lists | Chat | Security | About Us

- Surveillance
- Human Security
- Device Security
- Message Security
- Network Security
- Resources

Support Riseup!

Tags

security pgp gpg otr thunderbird Enigmail confidentiality

Related

- Encrypting email with Thunderbird
- Howto Setup OpenPGP Keys
- Secure Instant Messaging with OTR
- Chat Security
- Riseup Chat

Message Security

Message security is the practice of encrypting messages on your device so that they can be read only by the intended recipient. Although network security and device security are important, this kind of **message encryption** is necessary in many situations:

- **Confidentiality:** Message encryption is the only way to ensure that only the indented recipients are reading your messages.
- **Authenticity:** Message encryption is the only way to ensure the identity of the people you are communicating with.

Practicing message encryption, however, can be a challenge:

- **You must own a device:** The idea with message encryption is that you don't trust another party to encrypt your communication for you. Therefore, all the encryption takes place on your machine, which means you need to own your own device.
- **Steep learning curve:** In order to use encryption software correctly, you will need to spend a significant amount of time learning important encryption concepts like public keys, private keys, keyrings, etc.
- **Limited correspondents:** With message encryption, you can only communicate securely with other people using the same software.

Obviously, these guarantees of security don't apply if your device has been compromised.

Concepts in Message Encryption

What these help pages call "message encryption" is technically called "public-key cryptography". Here is how it works:

- **Private key:** Everyone has their own private key. As the name implies, this key must be kept private. You use this private key in order to read the encrypted messages sent to you.
- **Public key:** Everyone also has a public key. This key is often distributed far and wide. When someone wants to send you a secure message, they use your public key to encrypt it. Only the person with the corresponding private key will be able to decrypt it.

Tips for Learning Message Encryption

Although it provides the highest level of security, public-key encryption is still an adventure to use

https://help.riseup.net/en/message-security
https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

CryptoParty.

Party like it's December 31st, 1983

What is CryptoParty?

Attend a CryptoParty to learn and teach how to use basic cryptography tools. A CryptoParty is free, public and fun. People bring their computers, mobile devices, and a willingness to learn!

CryptoParty is a decentralized, global initiative to introduce the most basic cryptography software and the fundamental concepts of their operation to the general public, such as the Tor anonymity network, public key encryption (PGP/GPG), and OTR (Off The Record messaging). CryptoParties are free to attend, public, and commercially and politically non-aligned. (see the guiding principles)

- Where is the next party in your area ?
- How to run your own party?
- What to learn and what to teach
- How to spread the word!
- Checkout the Handbook

Edit

Follow us...

… on Twitter, app.net and Diaspora for announcements.

Edit

Contact

Edit this page more… Register Login

CryptoParty.

Party like it's December 31st, 1983

Recent changes Sitemap

Party! | Learn! | Discuss! | Organize! | Spread!

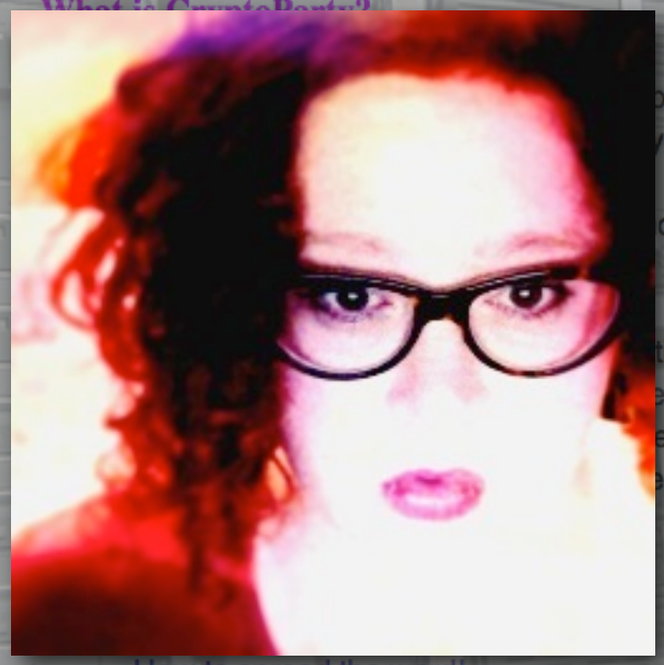


Table of Contents –

What is CryptoParty?

…toParty to learn and teach how to …yptography tools. A CryptoParty is … and fun. People bring their …obile devices, and a willingness to …

…tive to intro…ce the most basic cryptography software and the … general public, such as the Tor anonymity network, public key …ecord messaging). CryptoParties are free to attend, public, and … the guiding principles)

- How to spread the word!
- Checkout the Handbook

Follow us...

… on Twitter, app.net and Diaspora for announcements.

Contact

@Asher_Wolf

http://www.cryptoparty.in
https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

NSA-proof your e-mail in 2 hours

25 June 2013
by Drew Crawford

Published in:
Code

40 comments

You may be concerned that the NSA is reading your e-mail. Is there really anything you can do about it though? After all, you don't really want to move off of GMail / Google Apps. And no place you would host is any better.

Except, you know, hosting it yourself. The way that e-mail was *originally designed to work*. We've all just forgotten because, you know, webapps-n-stuff. It's a lot of work, mkay, and I'm a lazy software developer.

Today we kill your excuses. Because I'm going to show you exactly how to do it, it's going to take about two hours to set up, and it's a "set it and forget it" kind of setup. Not only that, but it is actually going to be **better** than GMail, from a purely features perspective. It might surprise you to learn that people continue to develop email server software in a post-Google-apps world, and that the state of self-hosted is much better than you remember.

Now fair warning: it took me about two days to figure the stuff out you're going to see in this blogpost, starting from knowing basically nothing about modern e-mail servers. But now that I've figured it out, if you don't ask too many questions you can implement it from these notes in just two hours. So take this not just as a guide for setting up an e-mail server, but as two days of free consulting, that just happens to produce a complete recipe for a modern, fully-featured, fast email server at the end. *You're really going to turn down free consulting? Come on, buckle down and do this.*

GitHub

This repository | Search or type a command

Explore Features Enterprise Blog

Sign up Sign in

PUBLIC al3x / sovereign

Star Fork

A set of Ansible playbooks to build and maintain your own private cloud: email, calendar, contacts, file sync, IRC bouncer, VPN, and more.

64 commits 1 branch 0 releases 7 contributors

branch: master sovereign /

Merge pull request #44 from greenalto/fix_whitespace ...

al3x authored 2 days ago latest commit 498719f034

roles	Merge pull request #44 from greenalto/fix_whitespace	2 days ago
README.textile	mention Roundcube in README	4 days ago
TODO	first commit	a month ago
Vagrantfile	Fix trailing whitespace in Vagrantfile	2 days ago
hosts	TODOs in hosts file	a month ago
requirements.txt	first commit	a month ago
site.yml	Merge branch 'master' of github.com:al3x/sovereign	3 days ago

README.textile

Code

Issues 13

Pull Requests 1

Pulse

Graphs

Network

HTTPS clone URL

https://github.com

You can clone with HTTPS, or Subversion.

Clone in Desktop

Download ZIP

https://tighub.com/al3x/sovereign/
https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

mailpile

A modern, fast web-mail client with user-friendly encryption and privacy features. 100% Free and Open Source software

---

We raised our $163,192 and 54 Bitcoins during our campaign

Thank you for your awesome support!

indiegogo

Bitcoin: **13z55AGS14pSPiPpMqAAFHb576tSmSmR77**

Press | Interface | Team | Features | Blog

Meet Our Team

Bjarni Einarsson
Tech Lead

Bjarni has been writing code and slinging servers since the mid-90s, including a 6 year stint fighting spam and viruses and 3 years behind the scenes on Google's site reliability team.

Smári McCarthy
Privacy & Security

Smári is the director of the **International Modern Media Institute**, a skilled programmer and a prominent member of the Icelandic Pirate Party.

He is also a sought after speaker who

Brennan Novak
Design & Front-end

Brennan Novak thrives on solving challenging interface design & user experience design problems.

Brennan has contracted for large companies like Nike & Intel, but prefers contributing his design &


https://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

THINGS TO THINK ABOUT

h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

1. SECURITY OF THE CONNECTION BETWEEN YOU AND YOUR EMAIL SERVICE (HTTPS, SSL)

2. SECURITY OF THE CONNECTION BETWEEN YOUR EMAIL SERVICE AND OTHER EMAIL SERVICES (SMTP-TLS)

3. SECURING THE CONTENT OF YOUR EMAIL (PGP (PRETTY GOOD PRIVACY), ENIGMAIL)

4. SECURING THE STORAGE OF YOUR EMAIL (DISK ENCRYPTION, OFFSHORE HOSTING)

https://pressfreedomfoundation.org/encryption-works h
ttps://secure.flickr.com/photos/getbutterfly/6317955134/sizes/l/

PARTING SHOT

https://secure.flickr.com/photos/91027340@N03/8980097949/sizes/h/in/photolist-eFxmiZ-cbtJhN-7YodnZ-cKPf55-a1AiZb-8gEv6Y-8gCefR-aihGz1-ai7a1o-9baJKp-dR5Uqj/

https://secure.flickr.com/photos/wiertz/6092000030/sizes/l/


But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise, except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences, or one who avoids a pain that produces no resultant pleasure? On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure other greater pleasures, or else he endures pains to avoid worse pains. But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise, except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences, or one who avoids a pain that produces no resultant pleasure? On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure other greater pleasures, or else he endures pains to avoid worse pains. But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I willBut I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise, except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences, or one who avoids a pain that produces no resultant pleasure? On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure other greater pleasures, or else he endures pains to avoid worse pains. But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise, except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences, or one who avoids a pain that produces no resultant pleasure? On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the

contact:

philcryer.com / @fak3r

slides:

bit.ly/pc-slides

thanks: