

YAHOO!

Our Response to Internet Surveillance

PRESENTED BY **Alex Stamos** | ICANN 51 Tech Day | October 13, 2014

What are we responding to?

What are we responding to?

- Government tapping of public networks

What are we responding to?

- Government tapping of public networks
- Government tapping of private networks

What are we responding to?

- Government tapping of public networks
- Government tapping of private networks
- Adversaries tapping local networks

What are we responding to?

- Government tapping of public networks
- Government tapping of private networks
- Adversaries tapping local networks
- Adversaries gaining access to user accounts

What are we responding to?

- Government tapping of public networks
- Government tapping of private networks
- Adversaries tapping local networks
- Adversaries gaining access to user accounts
- Certificate authorities behaving badly

Transport Encryption

Transport Encryption

Complete

- › TLS 1.2
- › ECDH(E)
- › AES-GCM
- › RSA 2048
- › HSTS (mostly)

Transport Encryption

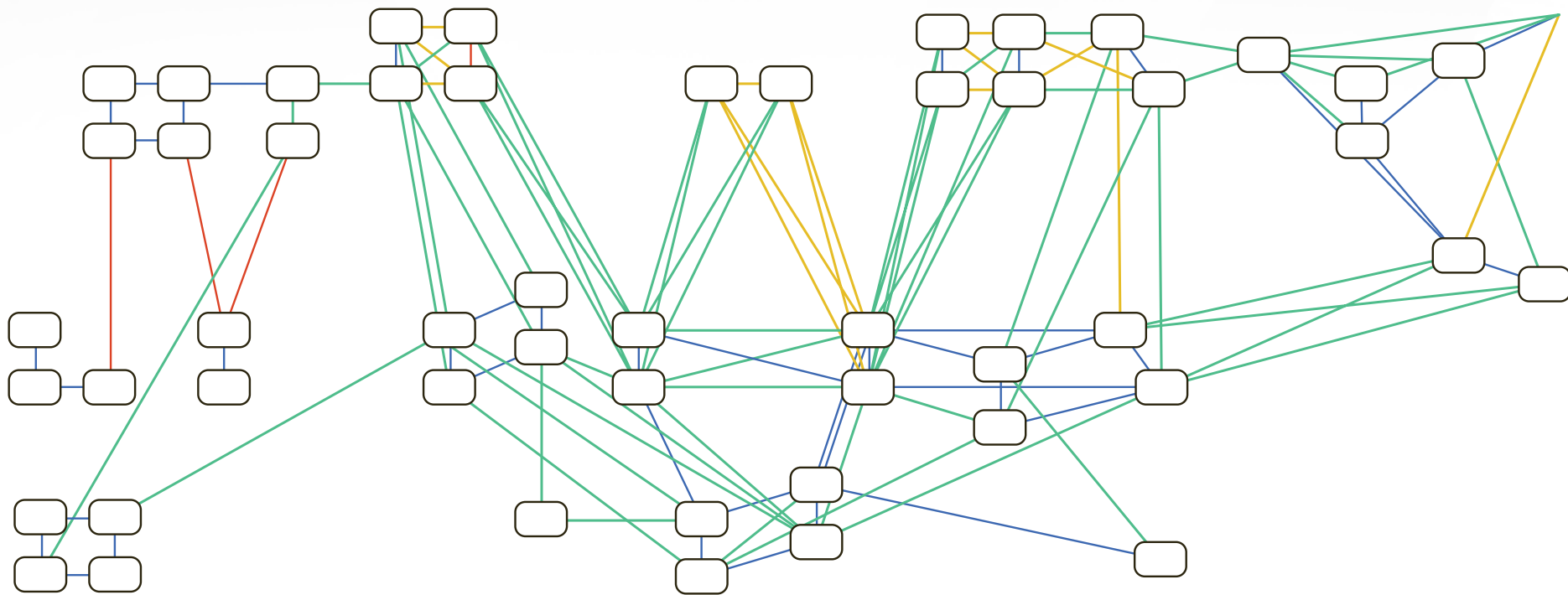
Complete

- › TLS 1.2
- › ECDH(E)
- › AES-GCM
- › RSA 2048
- › HSTS (mostly)

Next up

- › Pre-load pins
- › ECDSA certificates
- › Certificate Transparency
- › ChaCha20 and Poly1305
- › Our own ICA?

Backbone Encryption



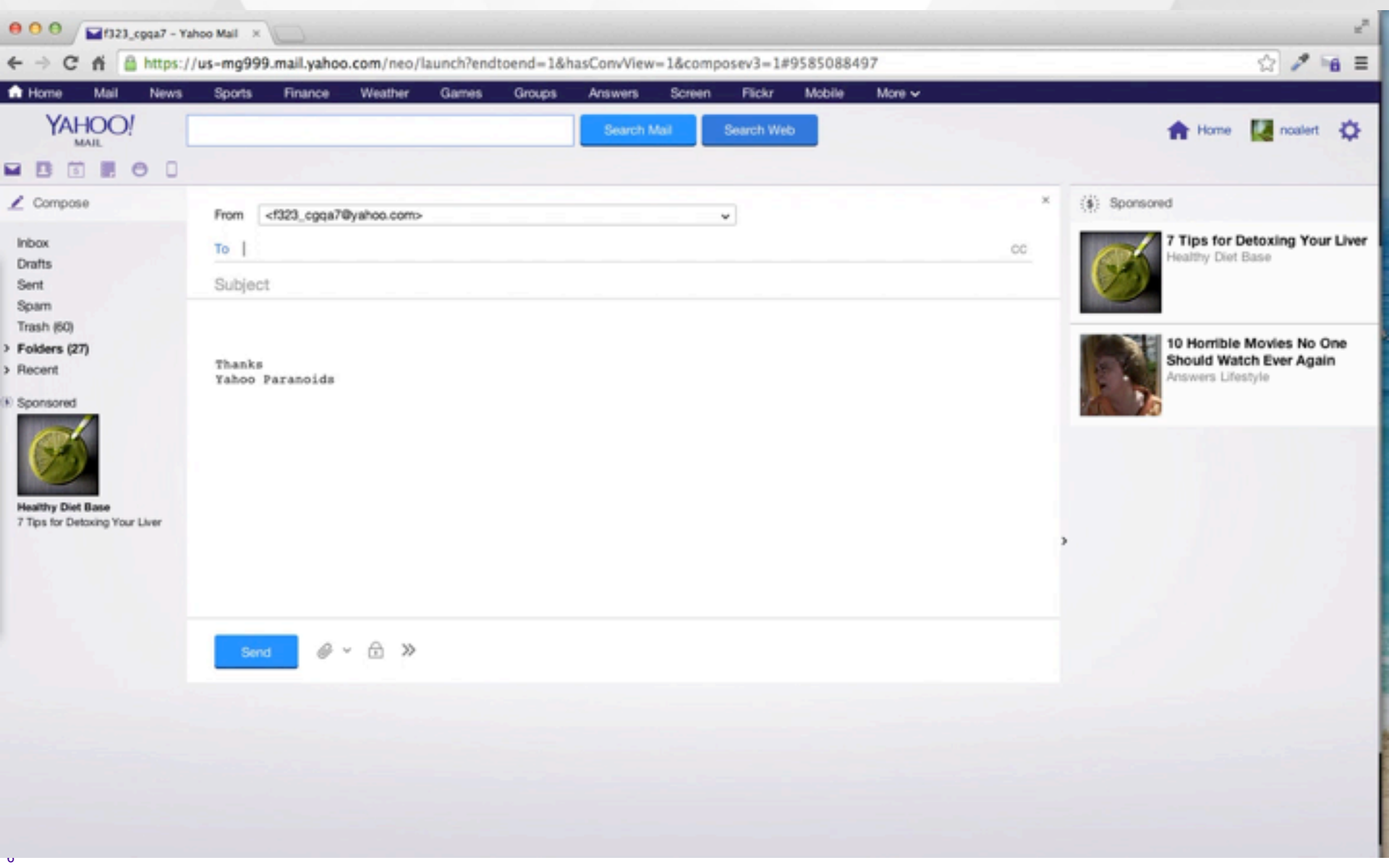
Self-Service Security

Self-Service Security

- Our scaling challenges in providing app sec services:
 - › Breadth: 80+ products in 60+ countries
 - › Speed: multiple daily web pushes and weekly mobile

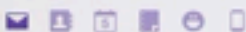
Self-Service Security

- Our scaling challenges in providing app sec services:
 - › Breadth: 80+ products in 60+ countries
 - › Speed: multiple daily web pushes and weekly mobile
- Any large org needs to create self-service options
 - › Mobile libraries
 - Authentication and device identity
 - TLS with pinning
 - › Mobile code scanning portal
 - › CI/CD Scanner integration
 - Open-source coming!



Search Mail

Search Web



Compose

- Inbox
- Drafts
- Sent
- Spam
- Trash (60)
- > Folders (27)
- > Recent
- Sponsored



Healthy Diet Base
7 Tips for Detoxing Your Liver

From <f323_cgqa7@yahoo.com>

To | CC

Subject

Thanks
Yahoo Paranoids

Send



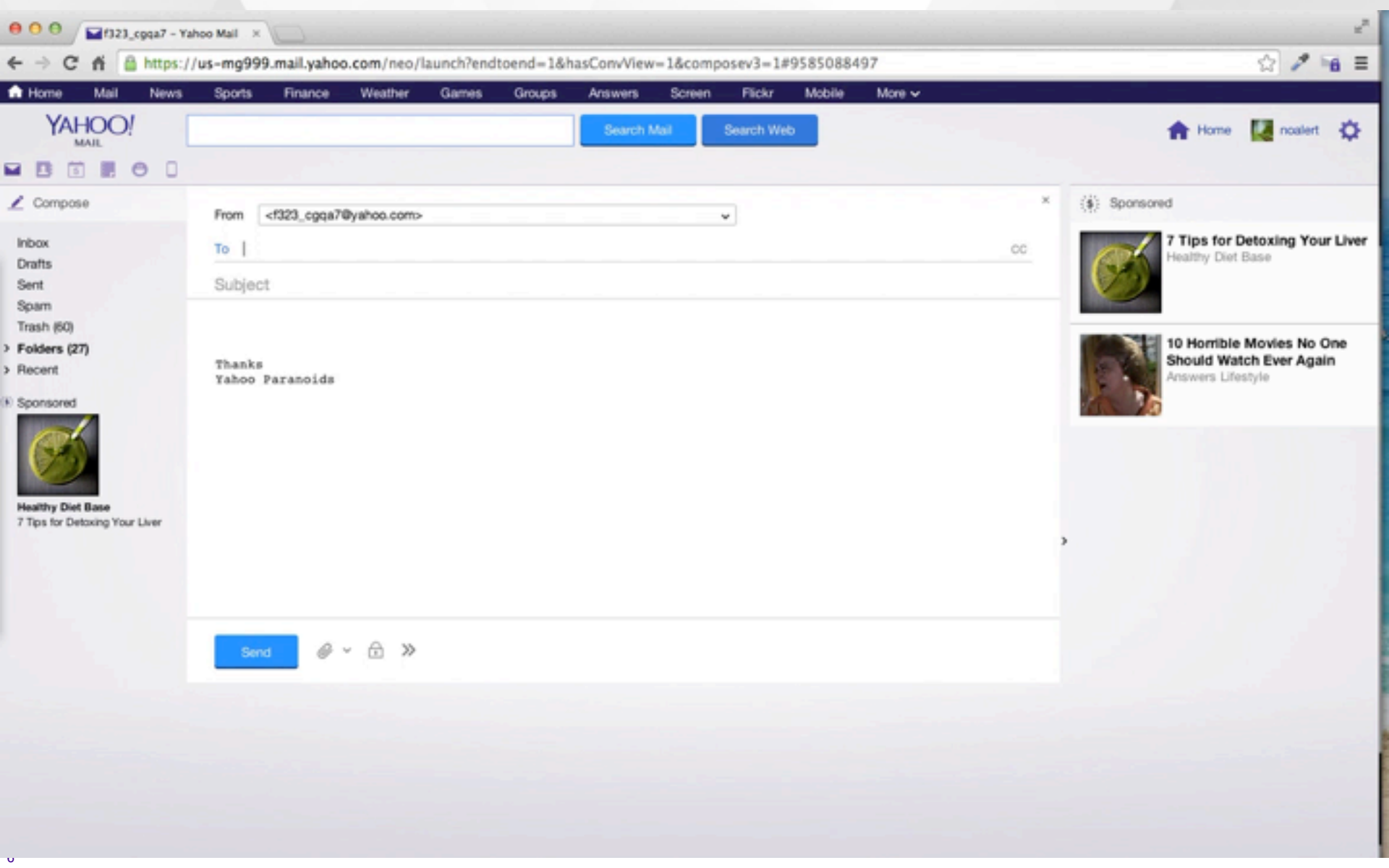
Sponsored



7 Tips for Detoxing Your Liver
Healthy Diet Base

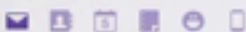


10 Horrible Movies No One
Should Watch Ever Again
Answers Lifestyle



Search Mail

Search Web



Compose

- Inbox
- Drafts
- Sent
- Spam
- Trash (60)
- > Folders (27)
- > Recent
- Sponsored



Healthy Diet Base
7 Tips for Detoxing Your Liver

From <f323_cgqa7@yahoo.com>

To | CC

Subject

Thanks
Yahoo Paranoids

Send

Sponsored



7 Tips for Detoxing Your Liver
Healthy Diet Base



10 Horrible Movies No One
Should Watch Ever Again
Answers Lifestyle

What else do we need?

What else do we need?

- Full non-NIST options
 - › Let's get ahead of the government mandates

What else do we need?

- Full non-NIST options
 - › Let's get ahead of the government mandates
- Pinning SMTP STARTTLS
 - › We do this on an ad-hoc basis, would love to see a standard

What else do we need?

- Full non-NIST options
 - › Let's get ahead of the government mandates
- Pinning SMTP STARTTLS
 - › We do this on an ad-hoc basis, would love to see a standard
- Opportunistic encryption in HTTP 2.0
 - › Making this optional is a huge mistake

What else do we need?

- Full non-NIST options
 - › Let's get ahead of the government mandates
- Pinning SMTP STARTTLS
 - › We do this on an ad-hoc basis, would love to see a standard
- Opportunistic encryption in HTTP 2.0
 - › Making this optional is a huge mistake
- A replacement for OpenPGP
 - › Flexible enough for multiple message types
 - › Modern ciphers, tiny message sizes
 - › Extensible with options like searchable encryption, FS ratcheting
 - › Key serving with zones of authority, CT-like proofing

DNSSEC: Help or Hinderance?

- The focus on DNSSEC is slowing down innovation in surveillance technologies
 - › Centralized keys
 - › Very uneven deployment
 - › Not end-to-end
- I would prefer to see more TOFU, opportunistic, and asymmetric solutions
- No solution in 2015 can centralize trust

Thank you

stamos@yahoo-inc.com