Fighting For Internet Security in the New Crypto Wars

Marcia Hofmann

Hack In the Box

May 28, 2015

“We’re in favor of strong encryption, robust encryption. The country needs it, industry needs it.

We just want to make sure we have a trap door and key under some judge’s authority where we can get there if someone is planning a crime."

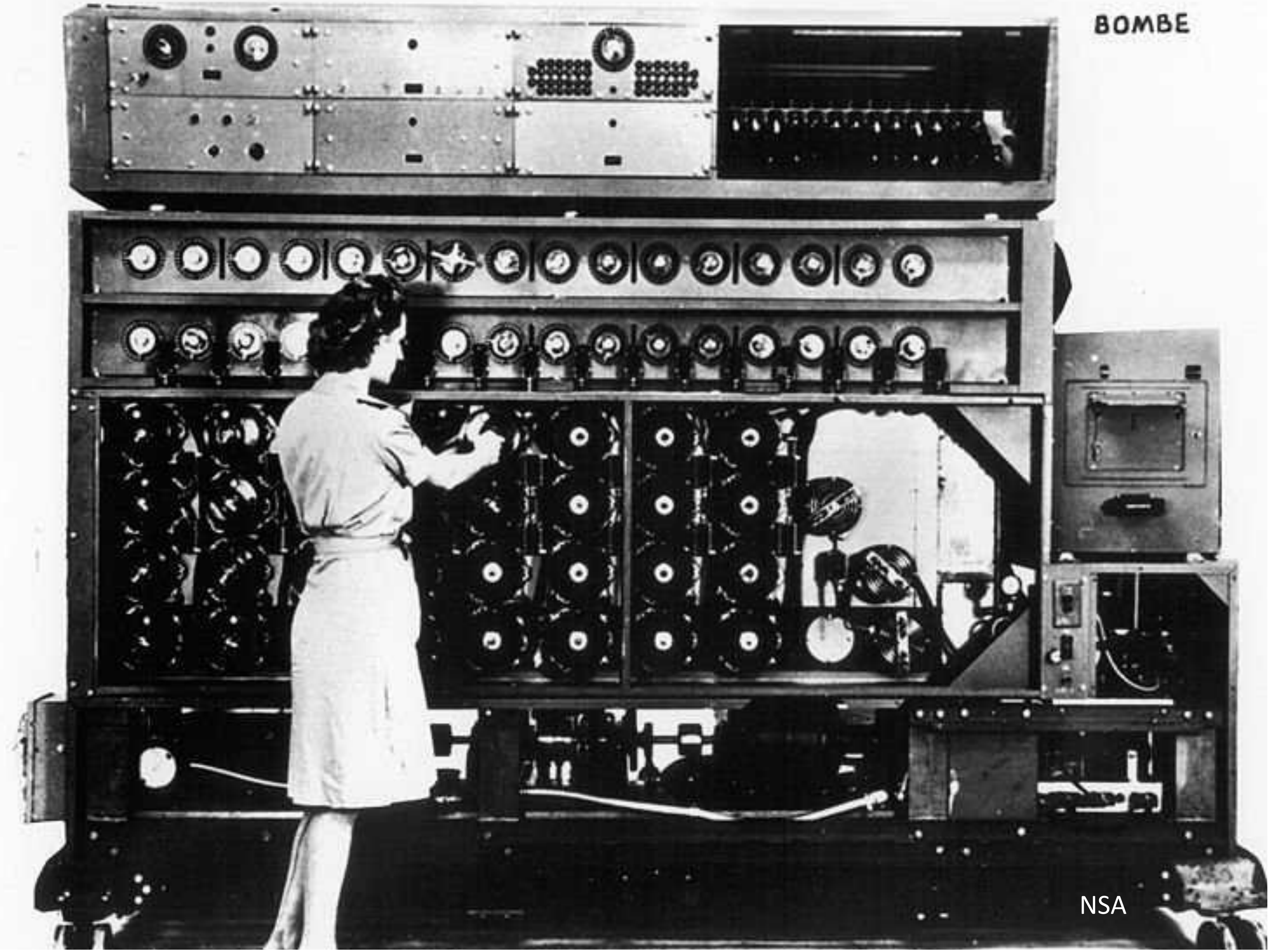
FBI Director Louis Freeh

1995

all of this has happened before,
and all of this will happen again

0.

prologue



NSA

Chuck Painter

Data Encryption Standard (DES)

1980s and early 1990s

- growing community of academic and private-sector researchers studying encryption
- rise of personal computers
- widespread adoption of the internet and advent of www

1980s and early 1990s

- increasingly digital telephone system
- flourishing of commercial technology
- for the first time, ordinary people could protect their communications and data

I.

the Crypto Wars of the ’90s

PGP

WIRED

HOW JOE BIDEN ACCIDENTALLY HELPED US ALL E-MAIL IN PRIVATE

key escrow

&

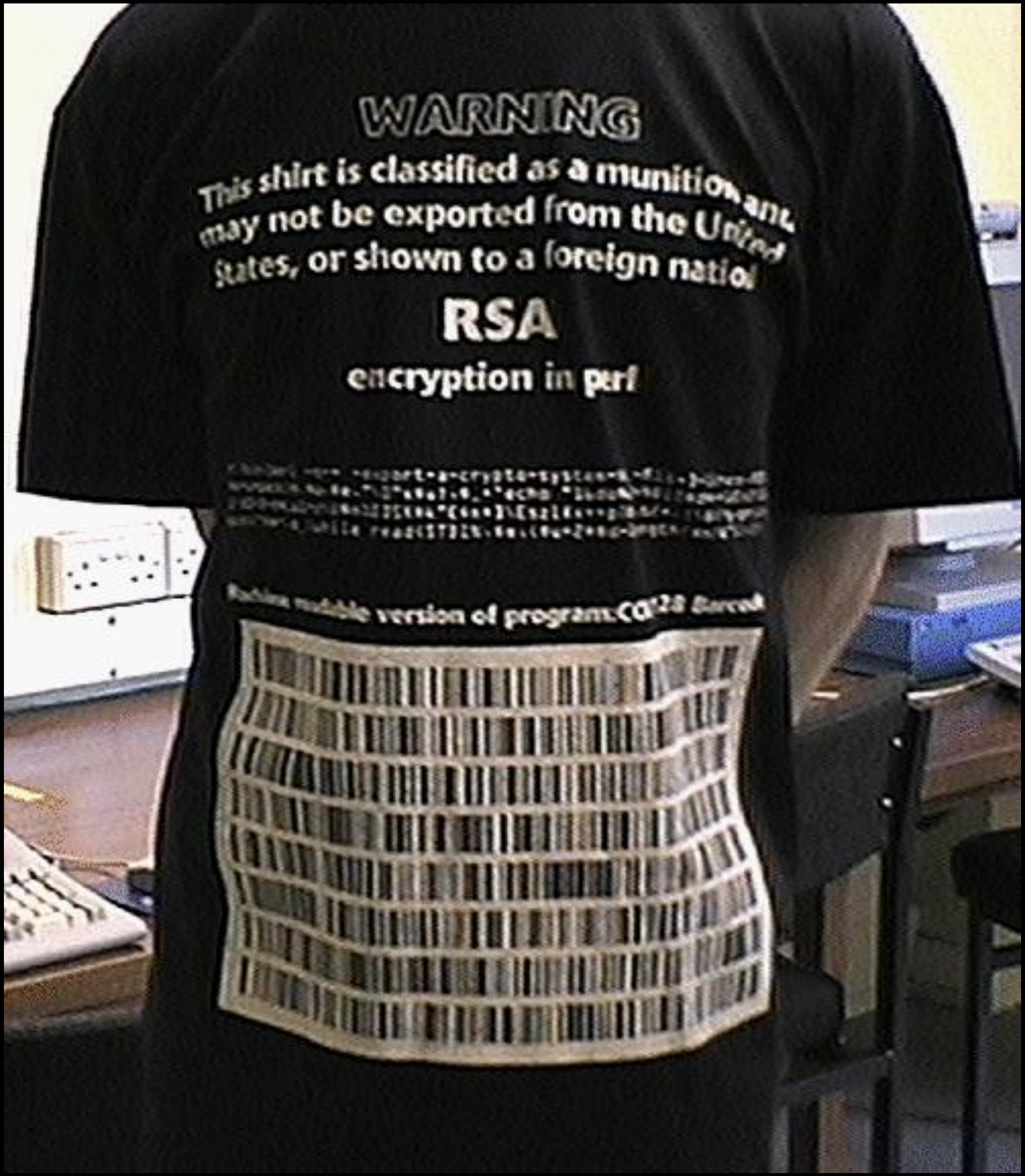
Clipper Chip

Matt Blaze

Communications Assistance for Law Enforcement Act

(CALEA)

export restrictions on encryption


WARNING
This shirt is classified as a munition and may not be exported from the United States, or shown to a foreign national
RSA
encryption in perl
Machine readable version of program: CODE128 Barcode

Adam Back

Wired Magazine

ceasefire

- intense pushback from tech industry
- intense pushback from public
- speculative law enforcement concerns
- government sense that export restrictions would prevent widespread adoption of encryption

2000s

- **global adoption of communication infrastructure**
- **globalization of tech companies**
- **intermediaries began storing vast amounts of user data**
- **mobile revolution**

II.

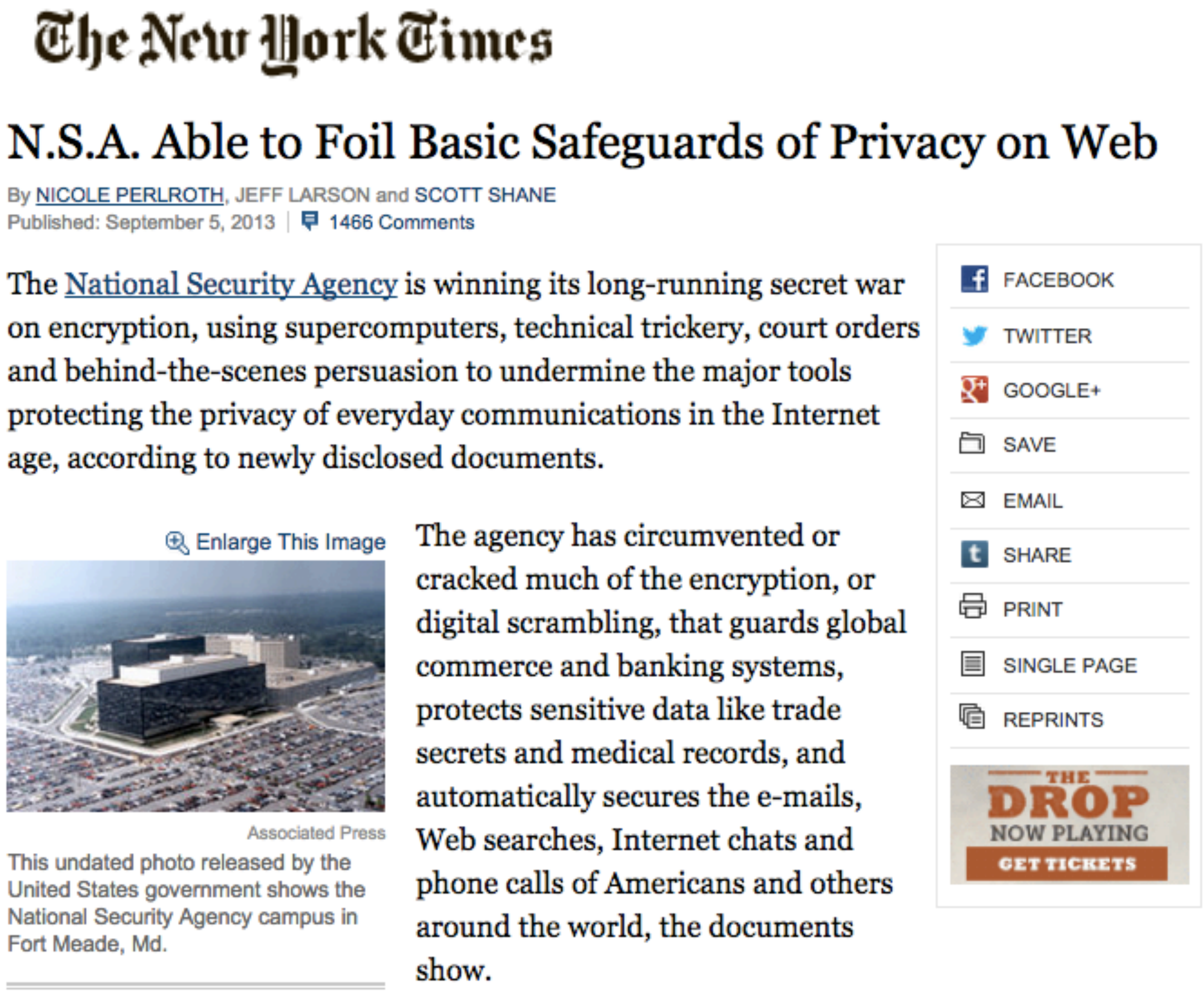
the Crypto Wars of the ‘10s

Tor
I Support Online Rights
ELECTRONIC FRONTIER FOUNDATION EFF.ORG

AP

government(s) as attacker(s)

BULLRUN



The New York Times

N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE

Published: September 5, 2013 | 1466 Comments

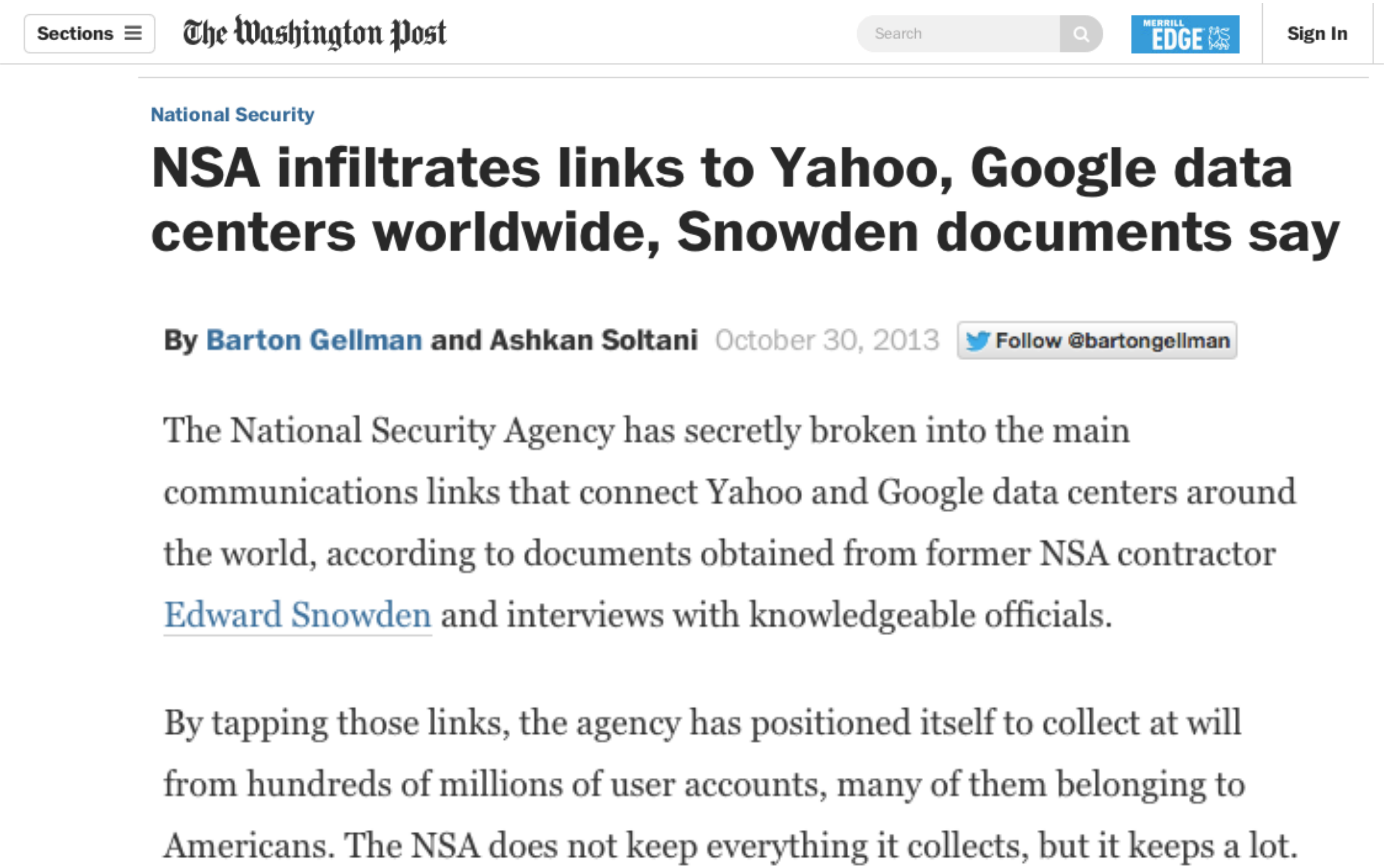
The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

Associated Press

This undated photo released by the United States government shows the National Security Agency campus in Fort Meade, Md.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

MUSCULAR



National Security

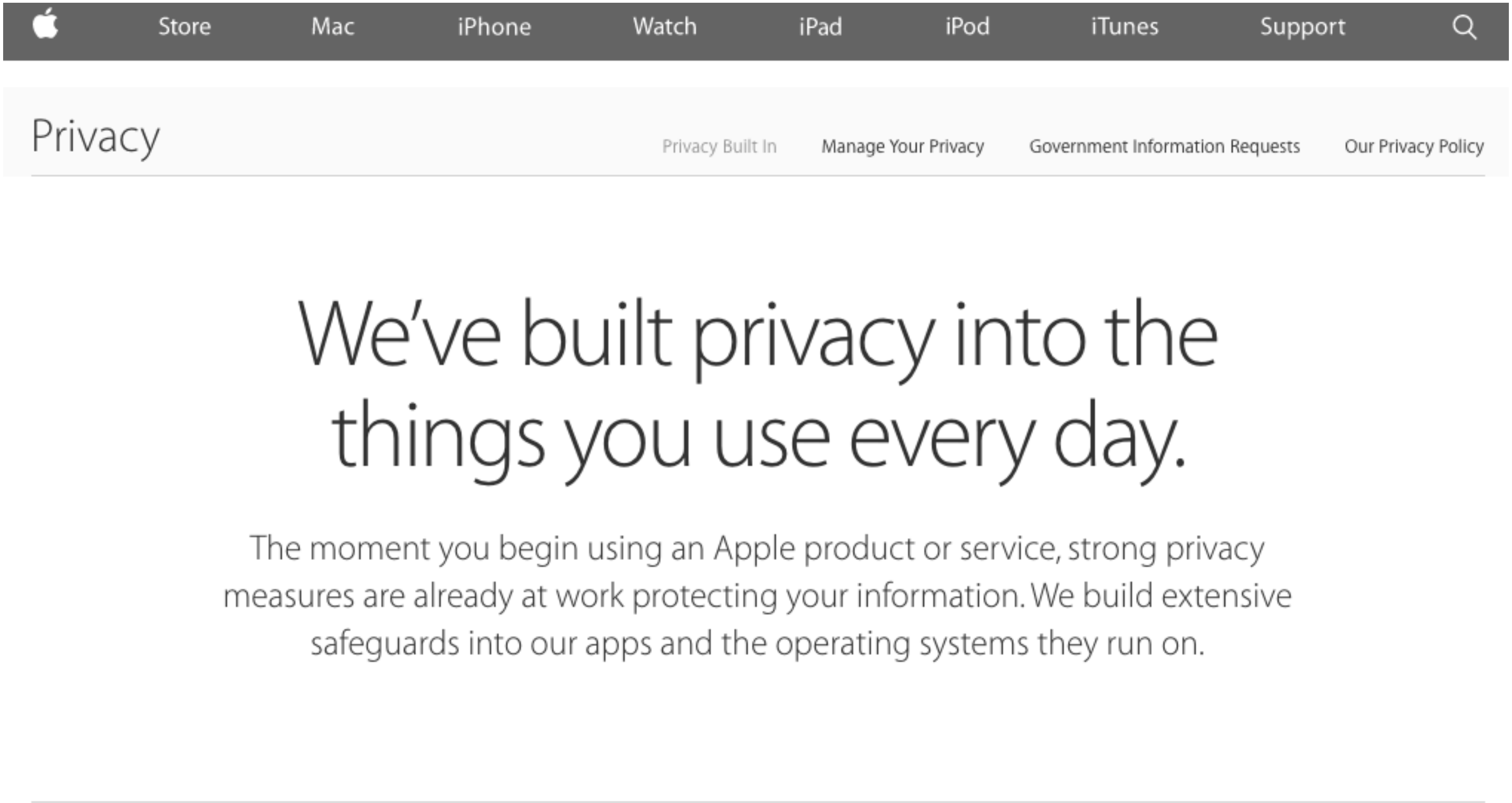
NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

By Barton Gellman and Ashkan Soltani October 30, 2013

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

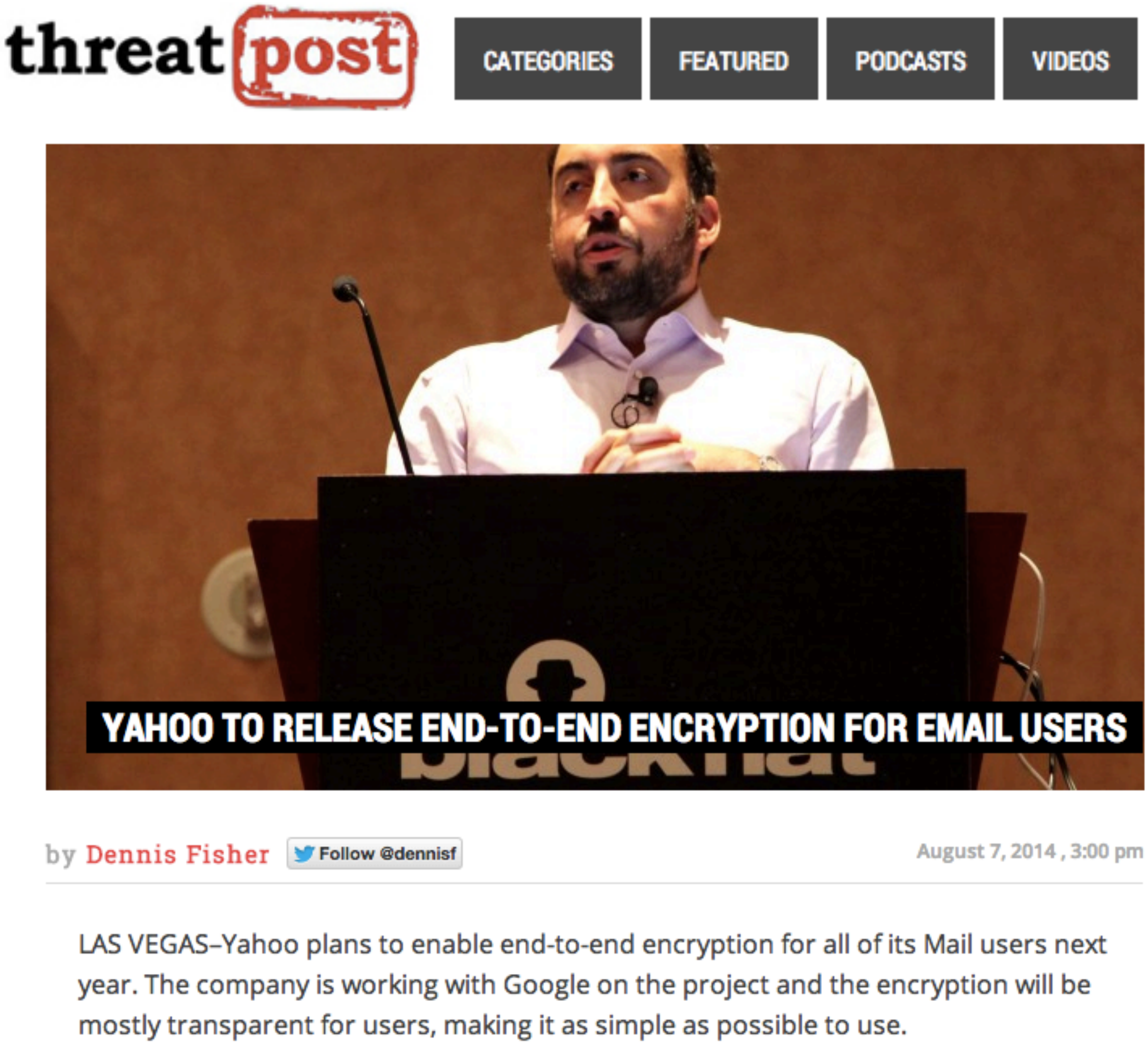
By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA does not keep everything it collects, but it keeps a lot.

Frederic Jacobs



We’ve built privacy into the things you use every day.

The moment you begin using an Apple product or service, strong privacy measures are already at work protecting your information. We build extensive safeguards into our apps and the operating systems they run on.

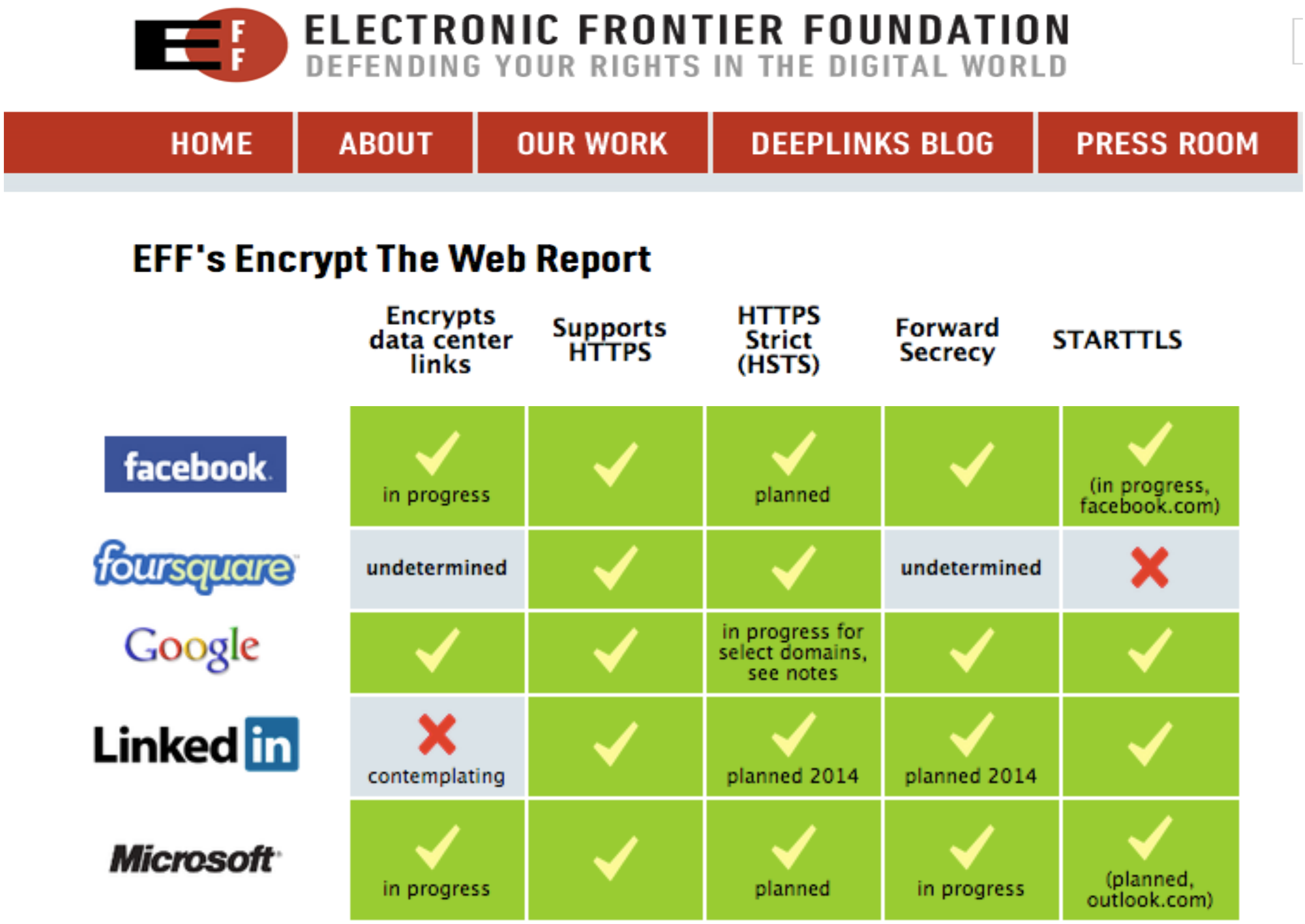


YAHOO TO RELEASE END-TO-END ENCRYPTION FOR EMAIL USERS

by Dennis Fisher

August 7, 2014 , 3:00 pm

LAS VEGAS–Yahoo plans to enable end-to-end encryption for all of its Mail users next year. The company is working with Google on the project and the encryption will be mostly transparent for users, making it as simple as possible to use.

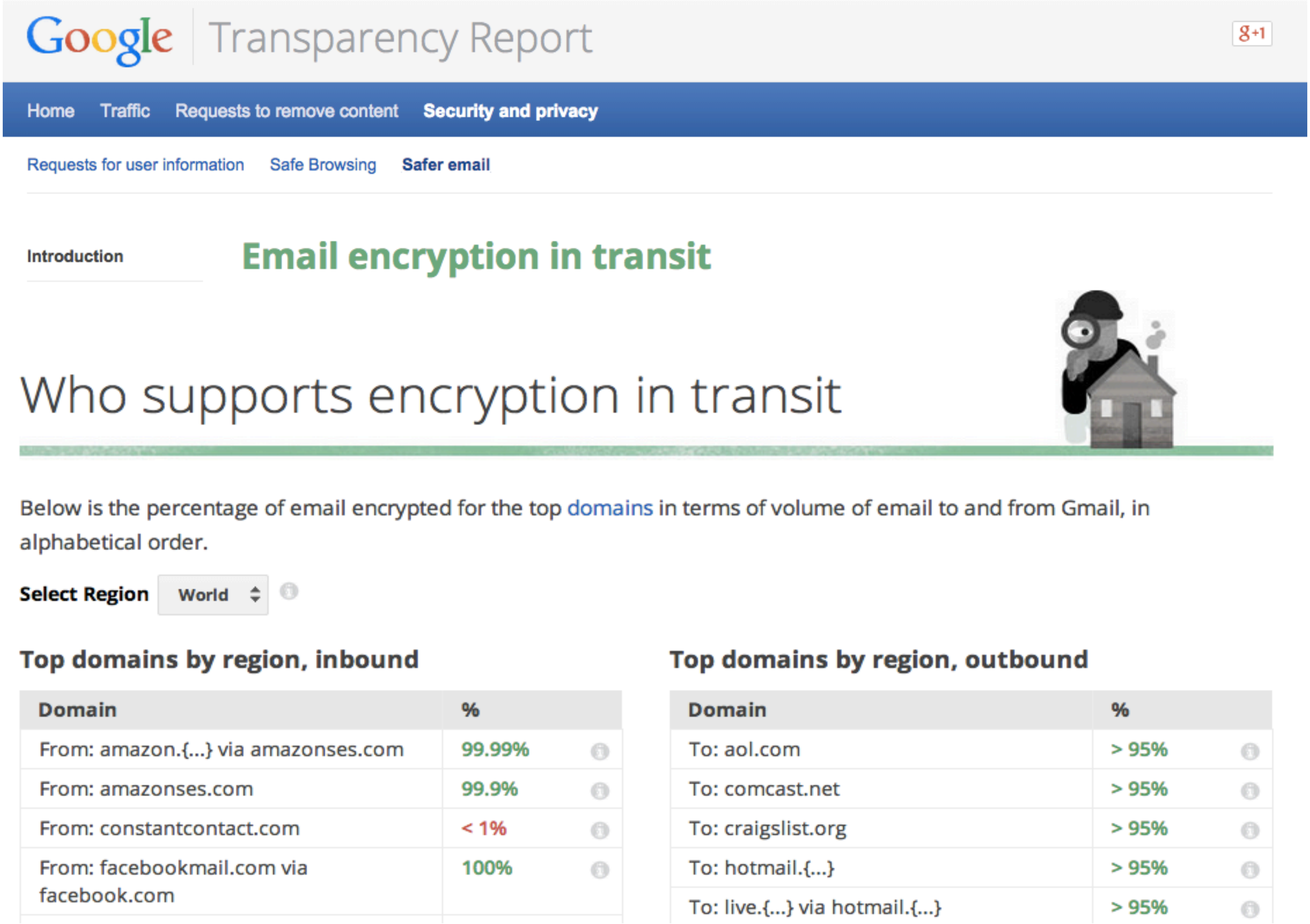


ELECTRONIC FRONTIER FOUNDATION

DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

EFF's Encrypt The Web Report

	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
facebook	✓ in progress	✓	✓ planned	✓	✓ (in progress, facebook.com)
foursquare	undetermined	✓	✓	undetermined	✗
Google	✓	✓	in progress for select domains, see notes	✓	✓
LinkedIn	✗ contemplating	✓	✓ planned 2014	✓ planned 2014	✓
Microsoft	✓ in progress	✓	✓ planned	✓ in progress	✓ (planned, outlook.com)



Google Transparency Report
g+1
Home
Traffic
Requests to remove content
Security and privacy
Requests for user information
Safe Browsing
Safer email
Introduction

Email encryption in transit

Who supports encryption in transit

Below is the percentage of email encrypted for the top domains in terms of volume of email to and from Gmail, in alphabetical order.

Select Region World

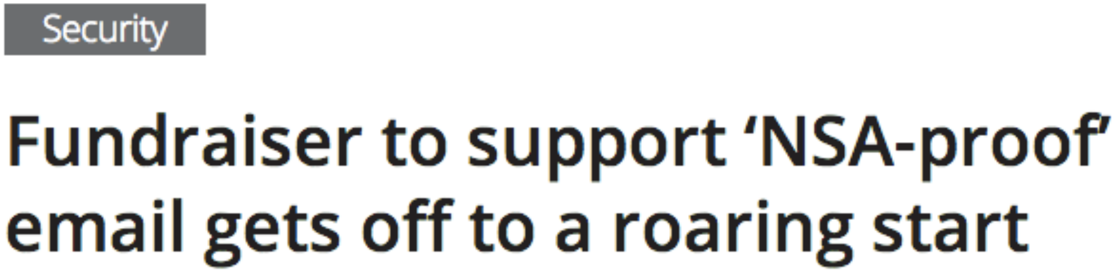
Top domains by region, inbound

Domain	%
From: amazon.{...} via amazonses.com	99.99%
From: amazonses.com	99.9%
From: constantcontact.com	< 1%
From: facebookmail.com via facebook.com	100%

Top domains by region, outbound

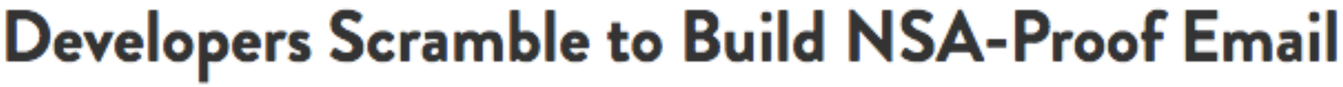
Domain	%
To: aol.com	> 95%
To: comcast.net	> 95%
To: craigslist.org	> 95%
To: hotmail.{...}	> 95%
To: live.{...} via hotmail.{...}	> 95%

Lavabit

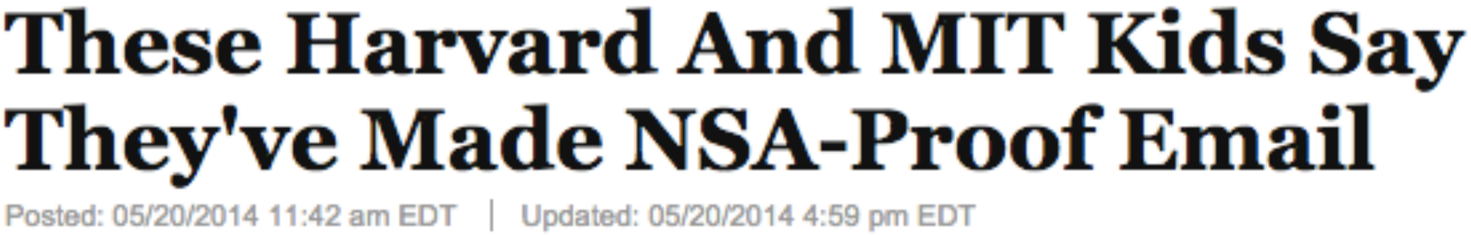


Security

Fundraiser to support 'NSA-proof' email gets off to a roaring start

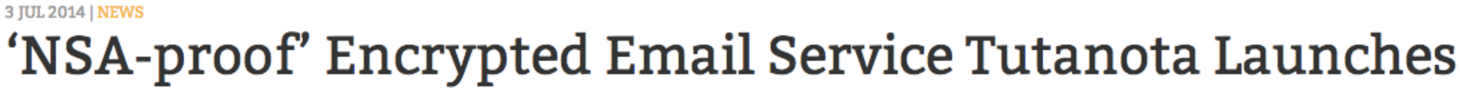


Developers Scramble to Build NSA-Proof Email



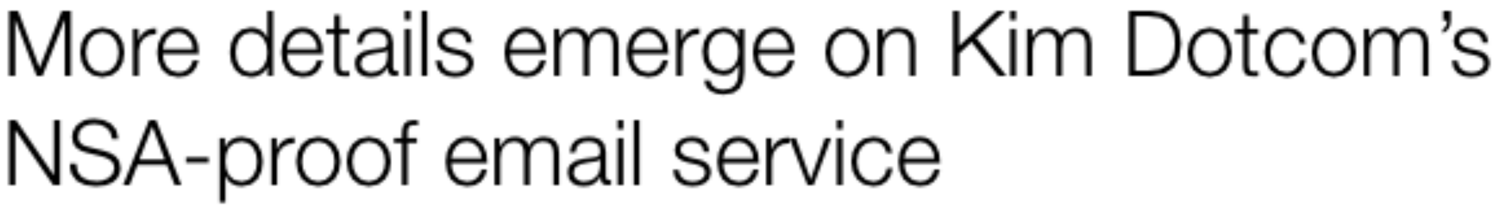
These Harvard And MIT Kids Say They've Made NSA-Proof Email

Posted: 05/20/2014 11:42 am EDT | Updated: 05/20/2014 4:59 pm EDT

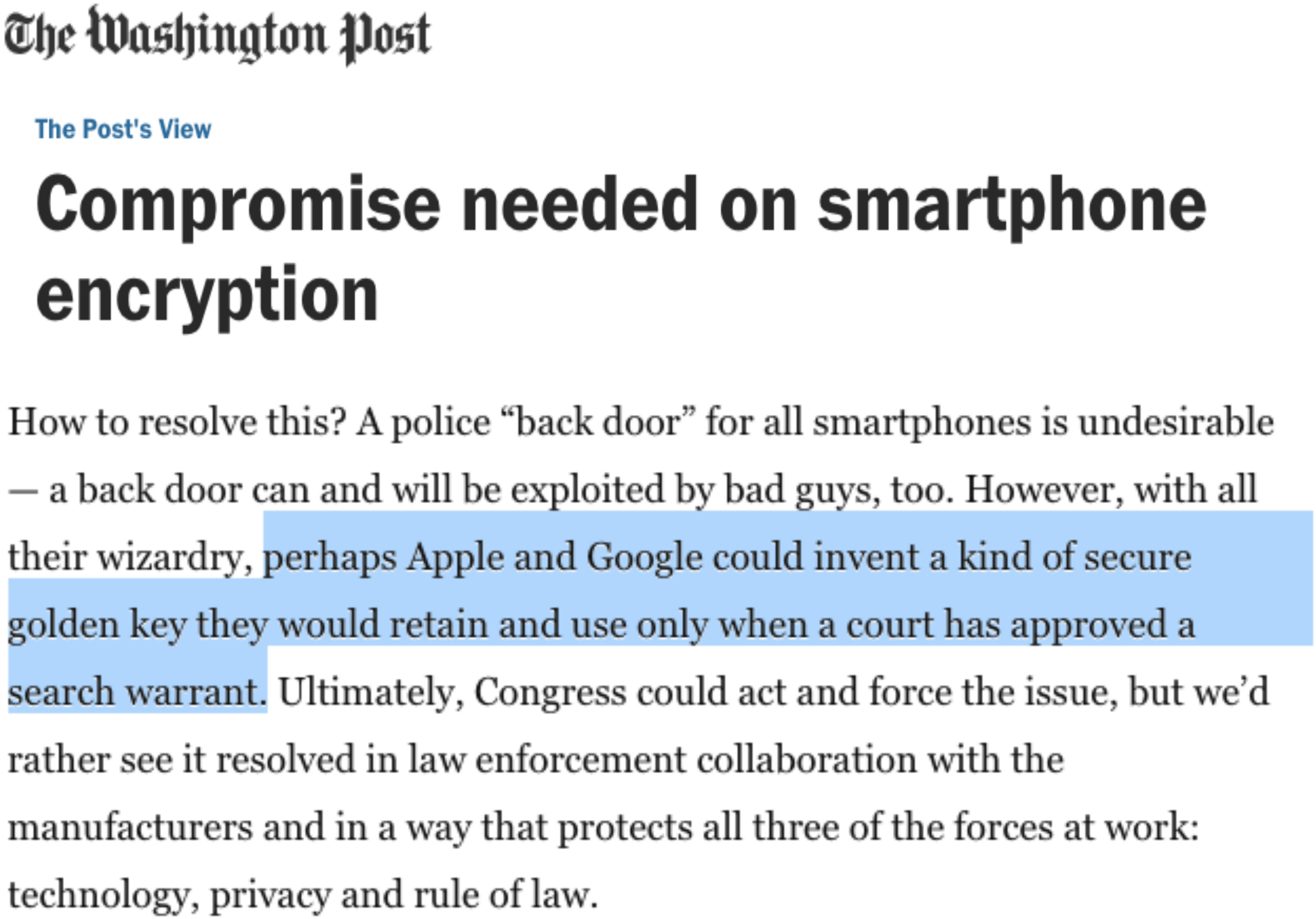


3 JUL 2014 | NEWS

'NSA-proof' Encrypted Email Service Tutanota Launches



More details emerge on Kim Dotcom's NSA-proof email service



The Washington Post

The Post's View

Compromise needed on smartphone encryption

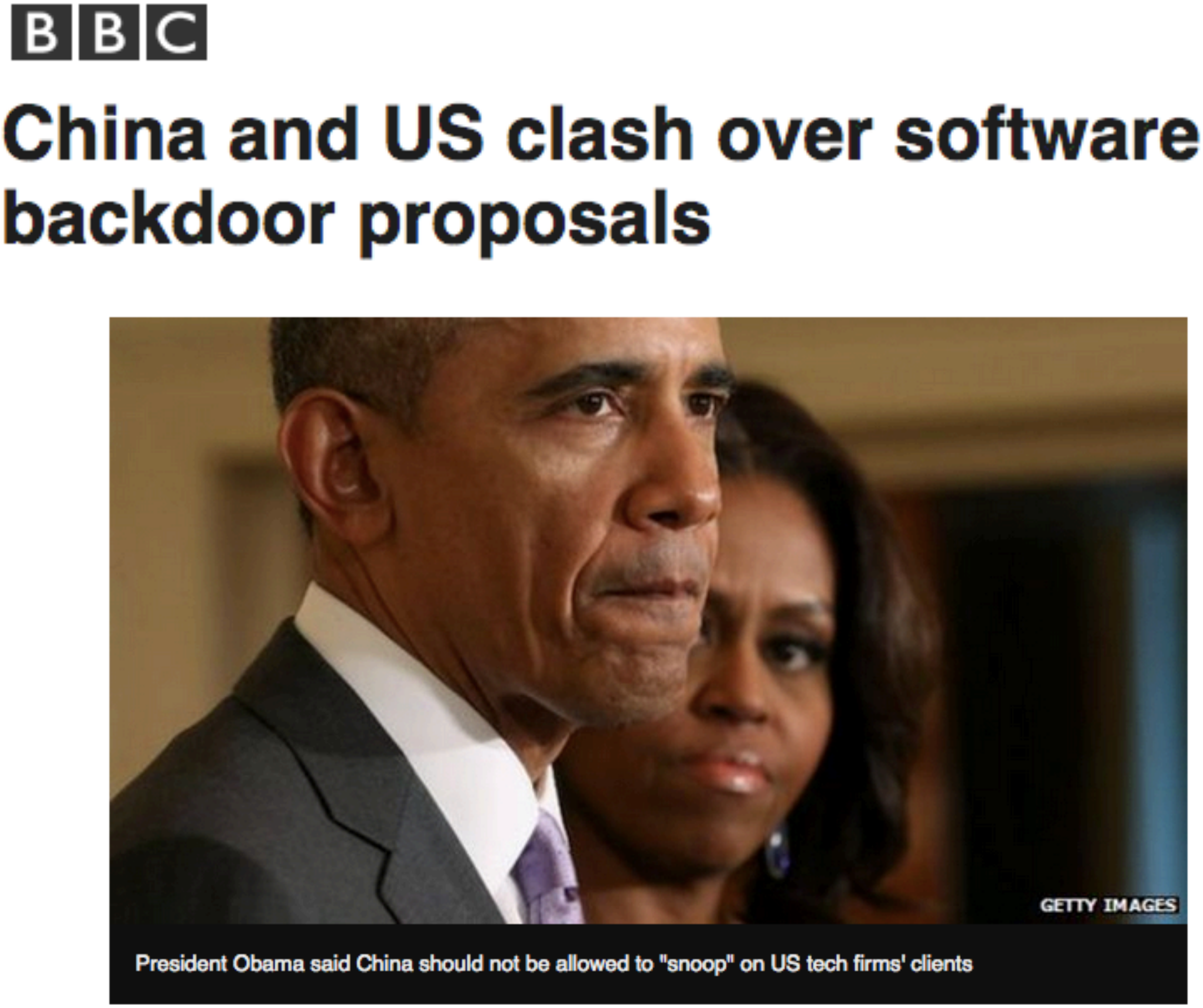
How to resolve this? A police “back door” for all smartphones is undesirable — a back door can and will be exploited by bad guys, too. However, with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant. Ultimately, Congress could act and force the issue, but we’d rather see it resolved in law enforcement collaboration with the manufacturers and in a way that protects all three of the forces at work: technology, privacy and rule of law.

The Washington Post

National Security

Tech giants don’t want Obama to give police access to encrypted phone data

FBI Director James B. Comey has expressed concern that the growing use of encrypted technologies is hindering the ability of law enforcement agencies to do their jobs. (Andrew Harnik/AP)



China and US clash over software backdoor proposals

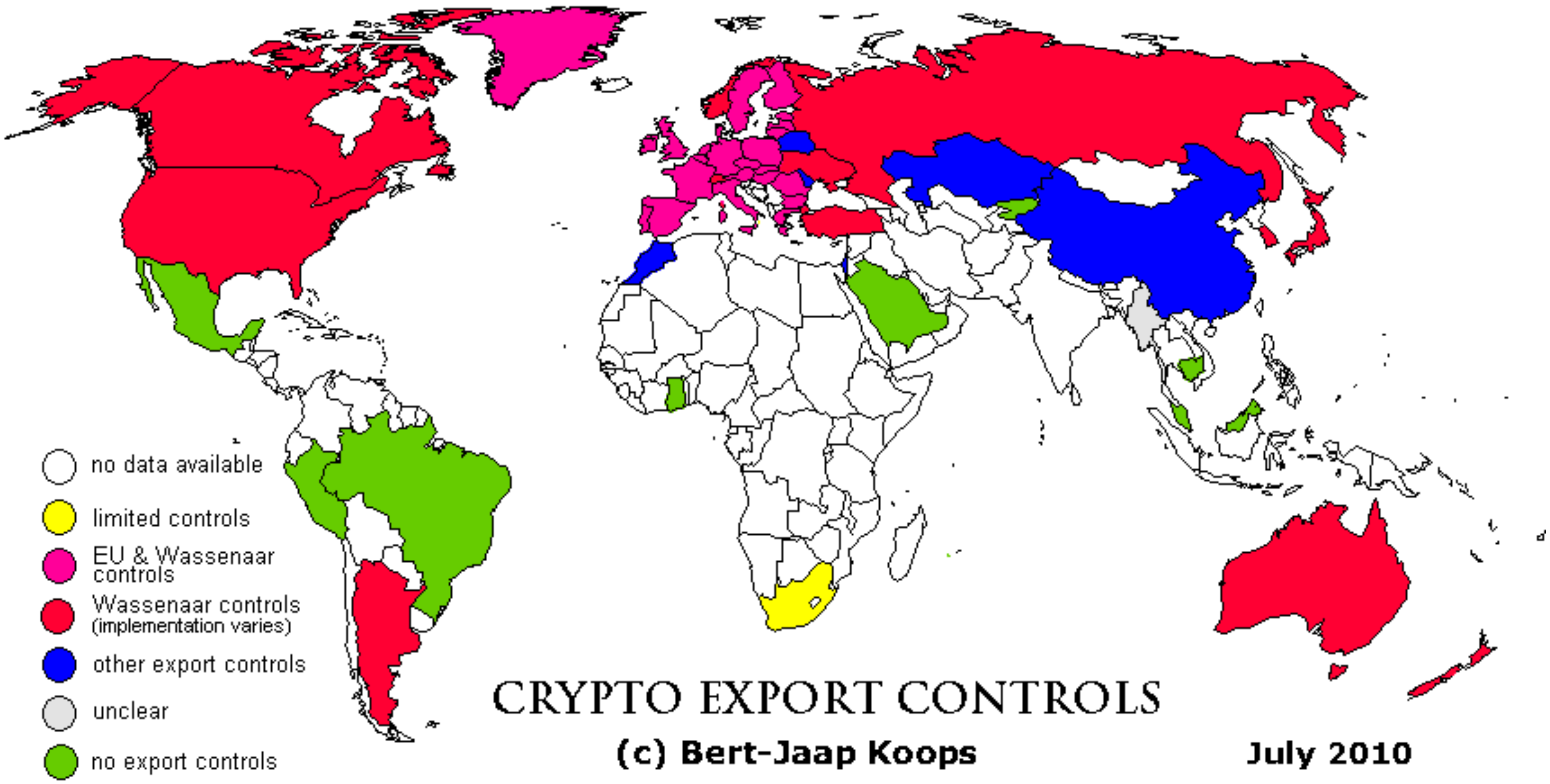
GETTY IMAGES

President Obama said China should not be allowed to "snoop" on US tech firms' clients

[redacted]

Wassenaar Arrangement

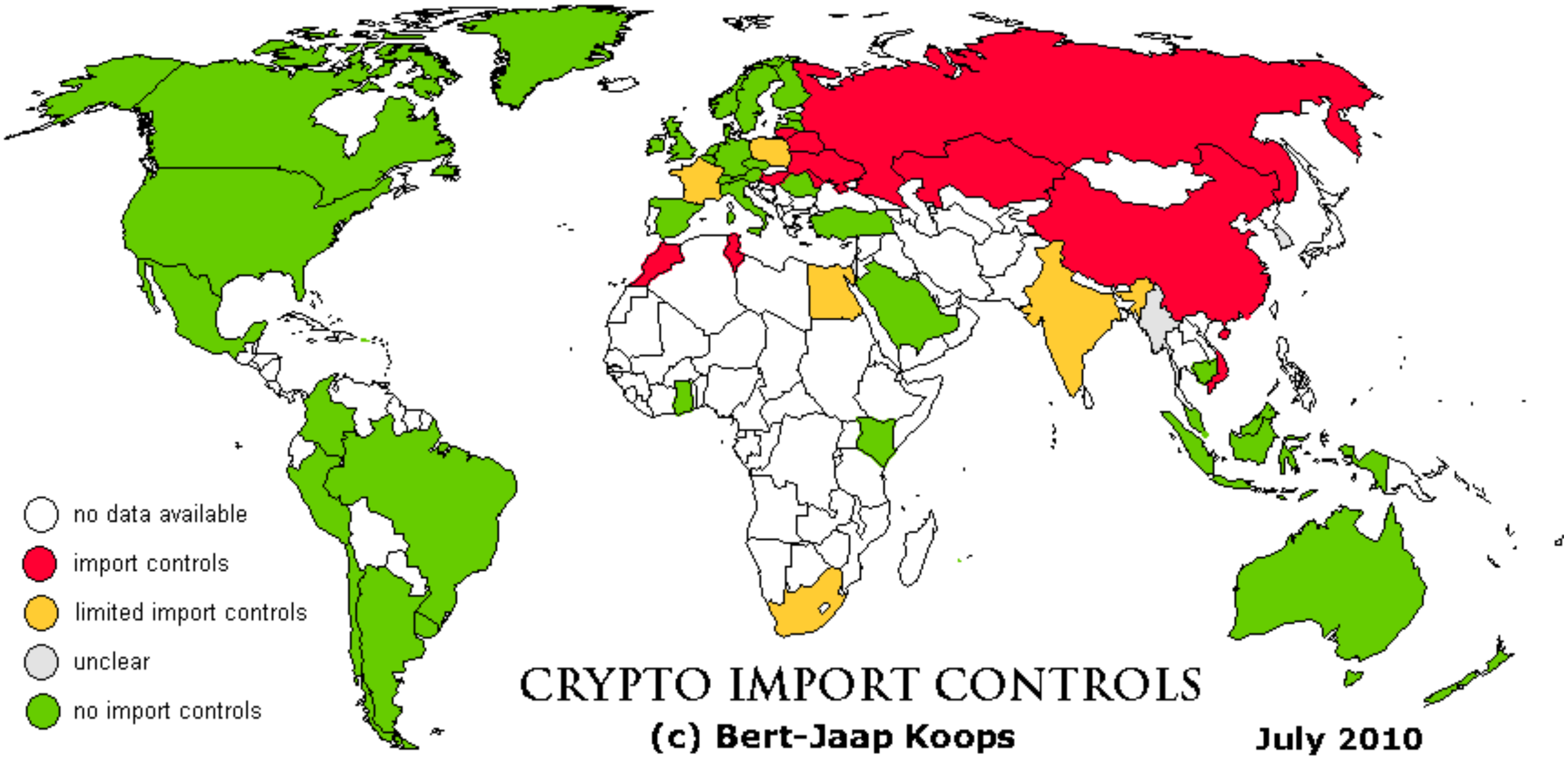
export restrictions on intrusion software and surveillance technology



CRYPTO EXPORT CONTROLS

(c) Bert-Jaap Koops

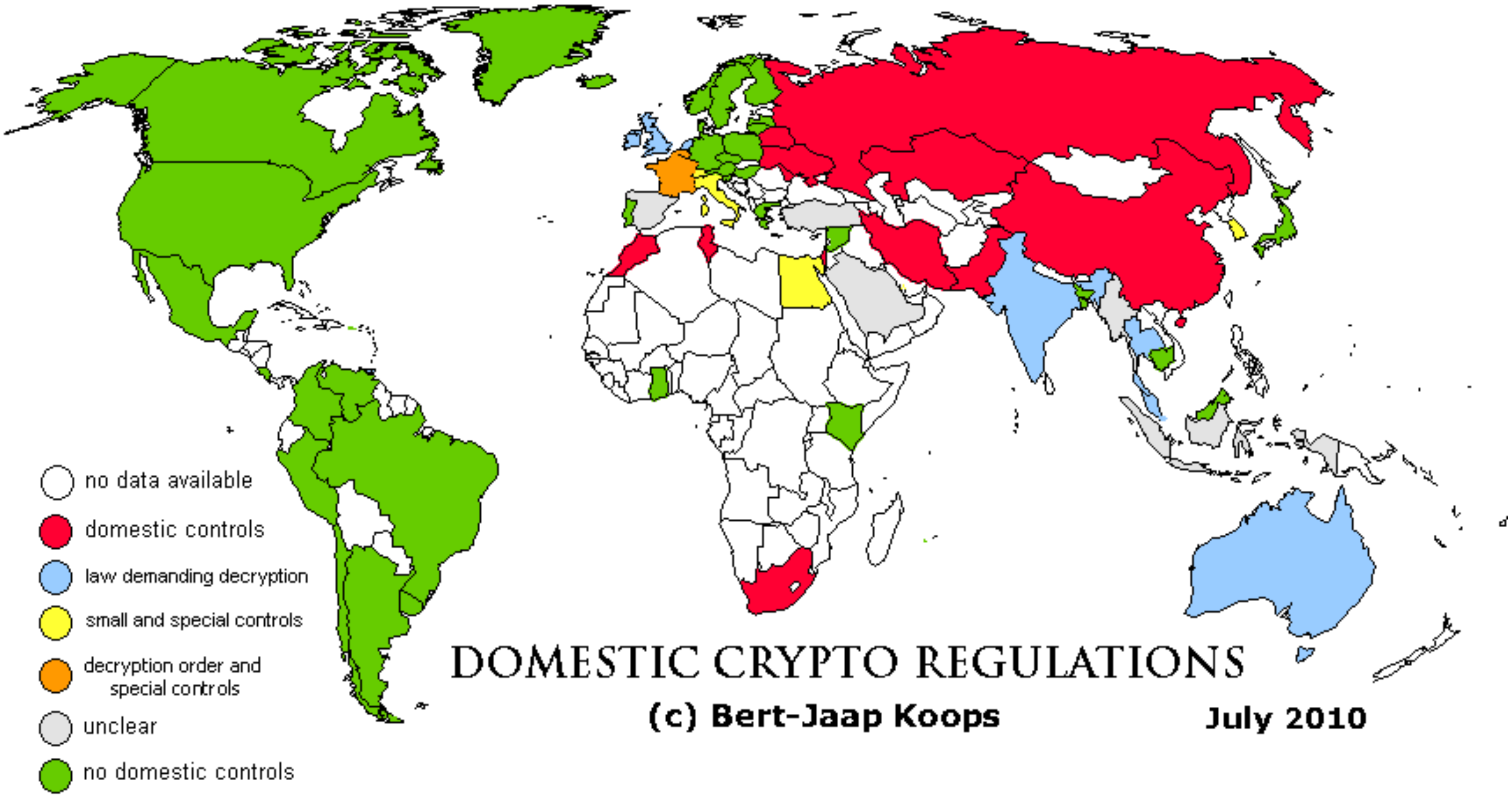
July 2010



CRYPTO IMPORT CONTROLS

(c) Bert-Jaap Koops

July 2010



○ no data available
🟥 domestic controls
🟦 law demanding decryption
🟨 small and special controls
🟧 decryption order and special controls
⬜ unclear
🟩 no domestic controls

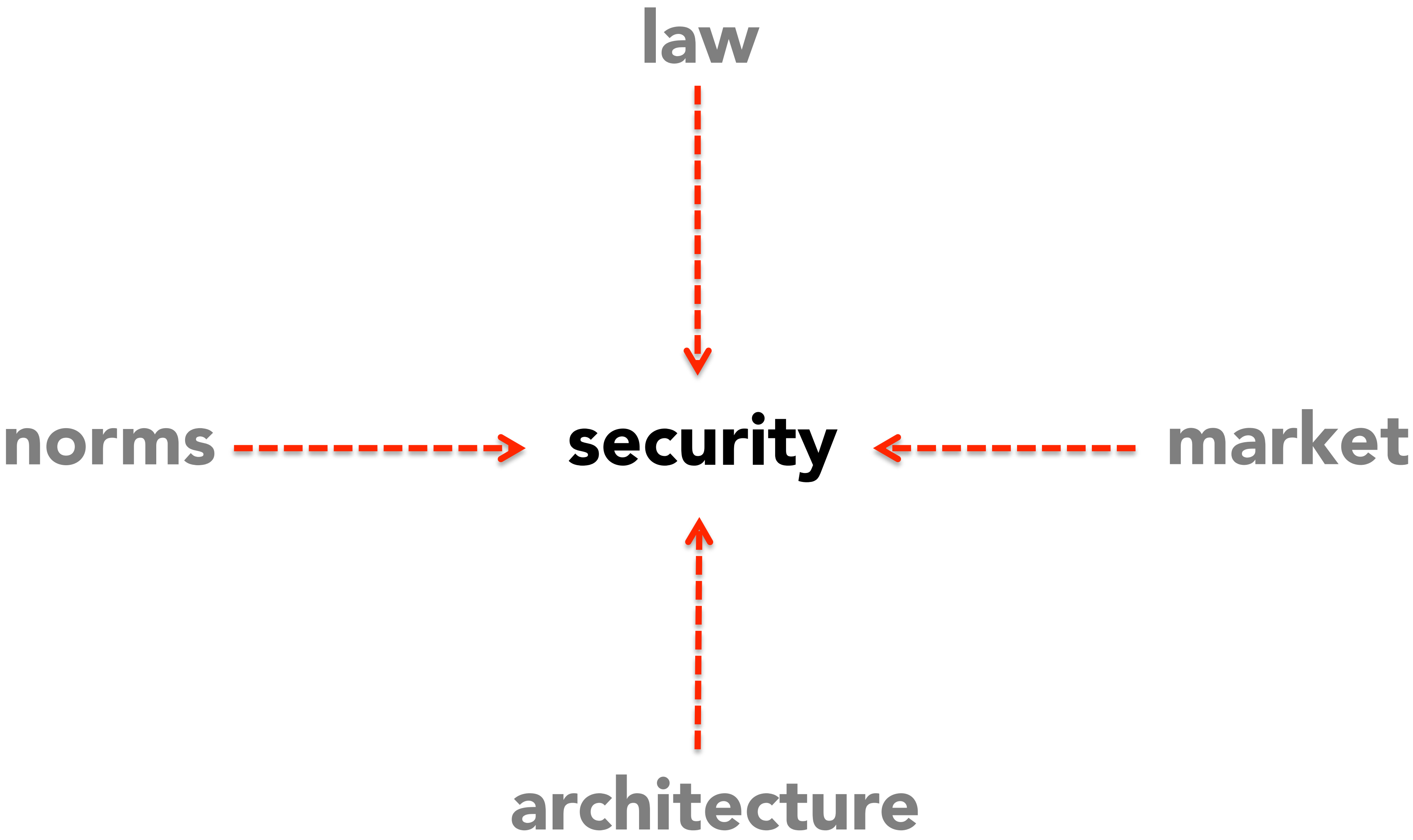
DOMESTIC CRYPTO REGULATIONS

(c) Bert-Jaap Koops July 2010

IV.

the future: what might happen? what should we do?

E
S
N
W
315



law

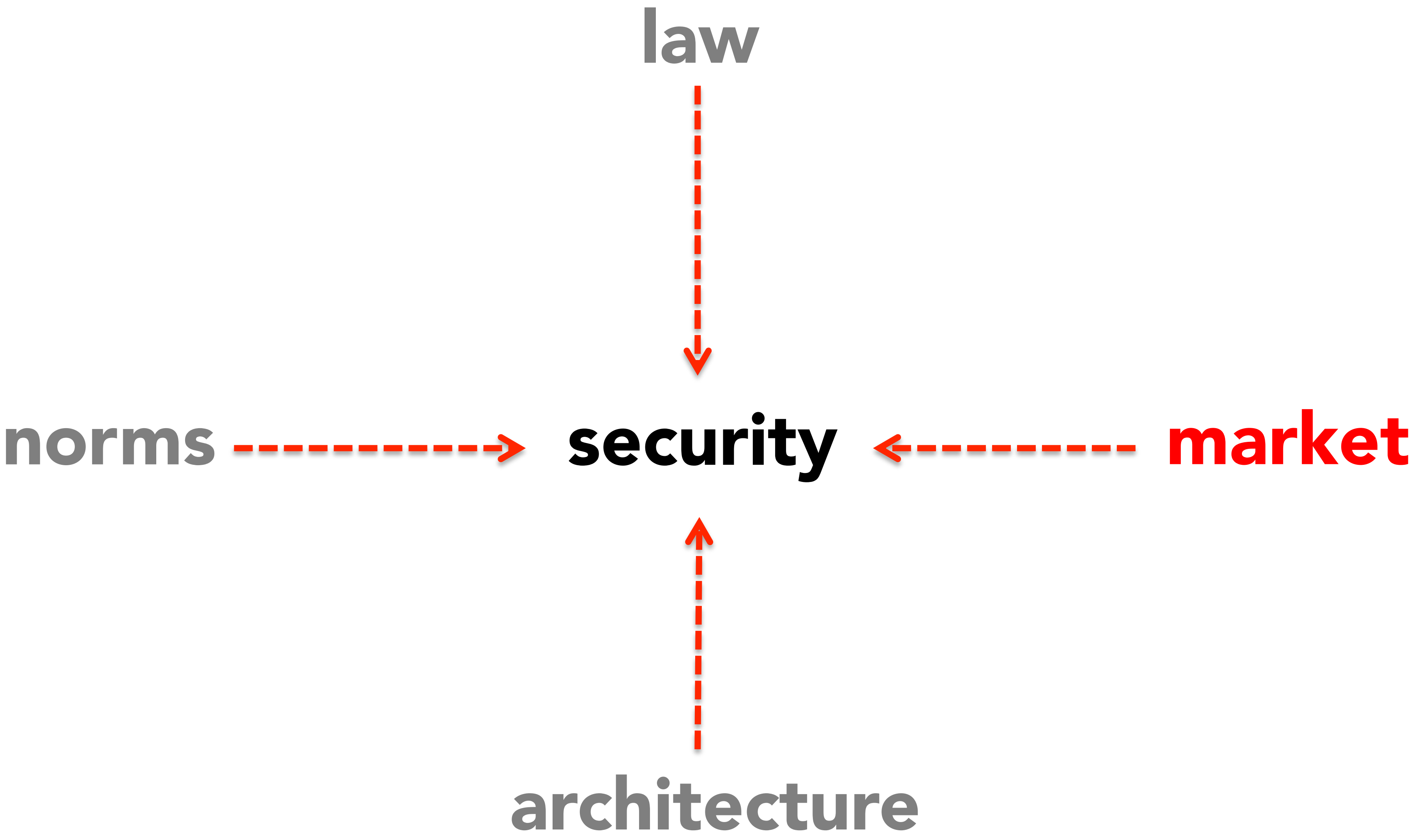
norms

security

market

architecture

Lawrence Lessig, Code and Other Laws of Cyberspace



law

norms

security

market

architecture

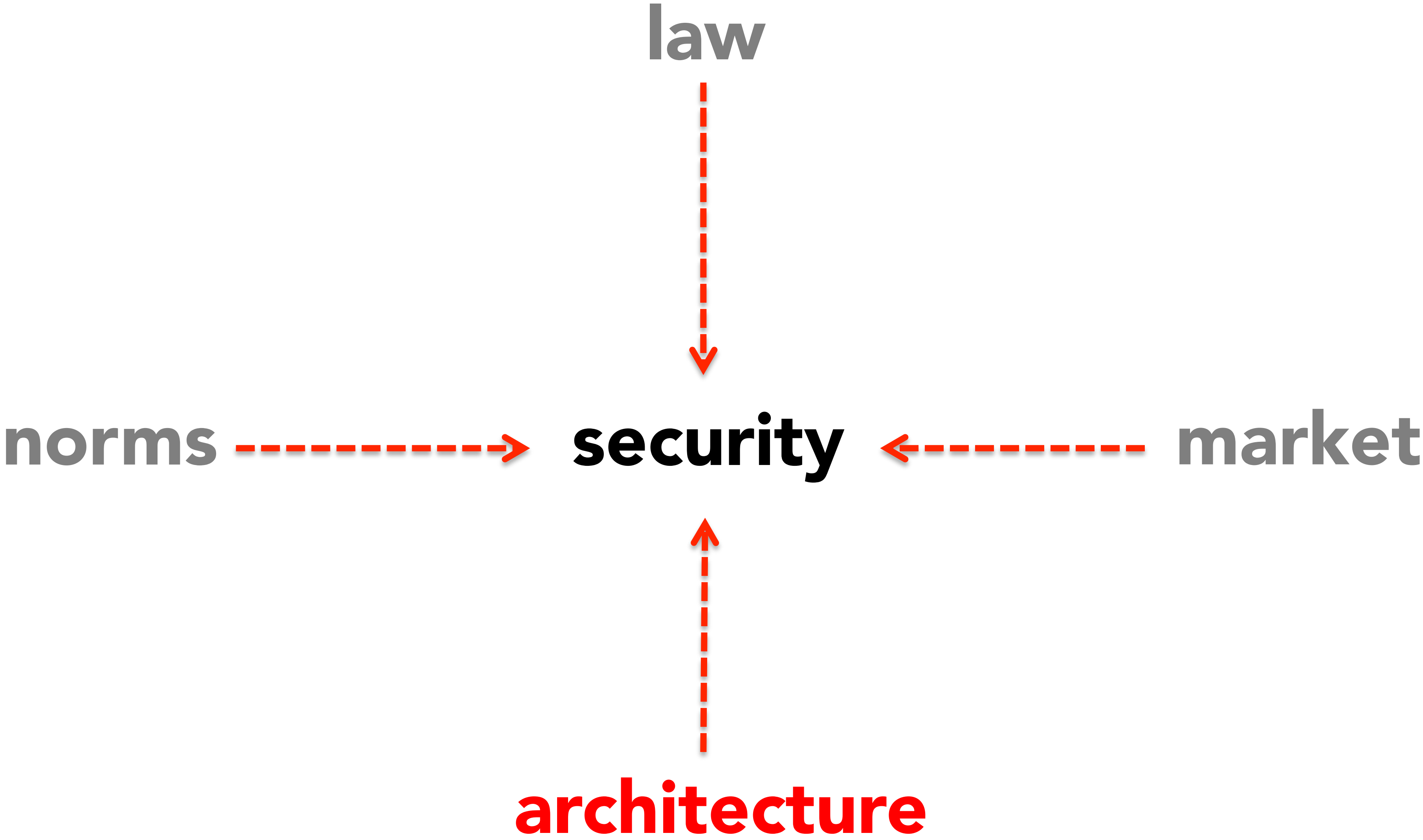
Lawrence Lessig, Code and Other Laws of Cyberspace

a major shift in
industry standards

privacy and security as a selling point

possible re-assessment of business models

possible business opportunities in encryption-friendly countries



law

norms

security

market

architecture

Lawrence Lessig, Code and Other Laws of Cyberspace

stronger, better crypto

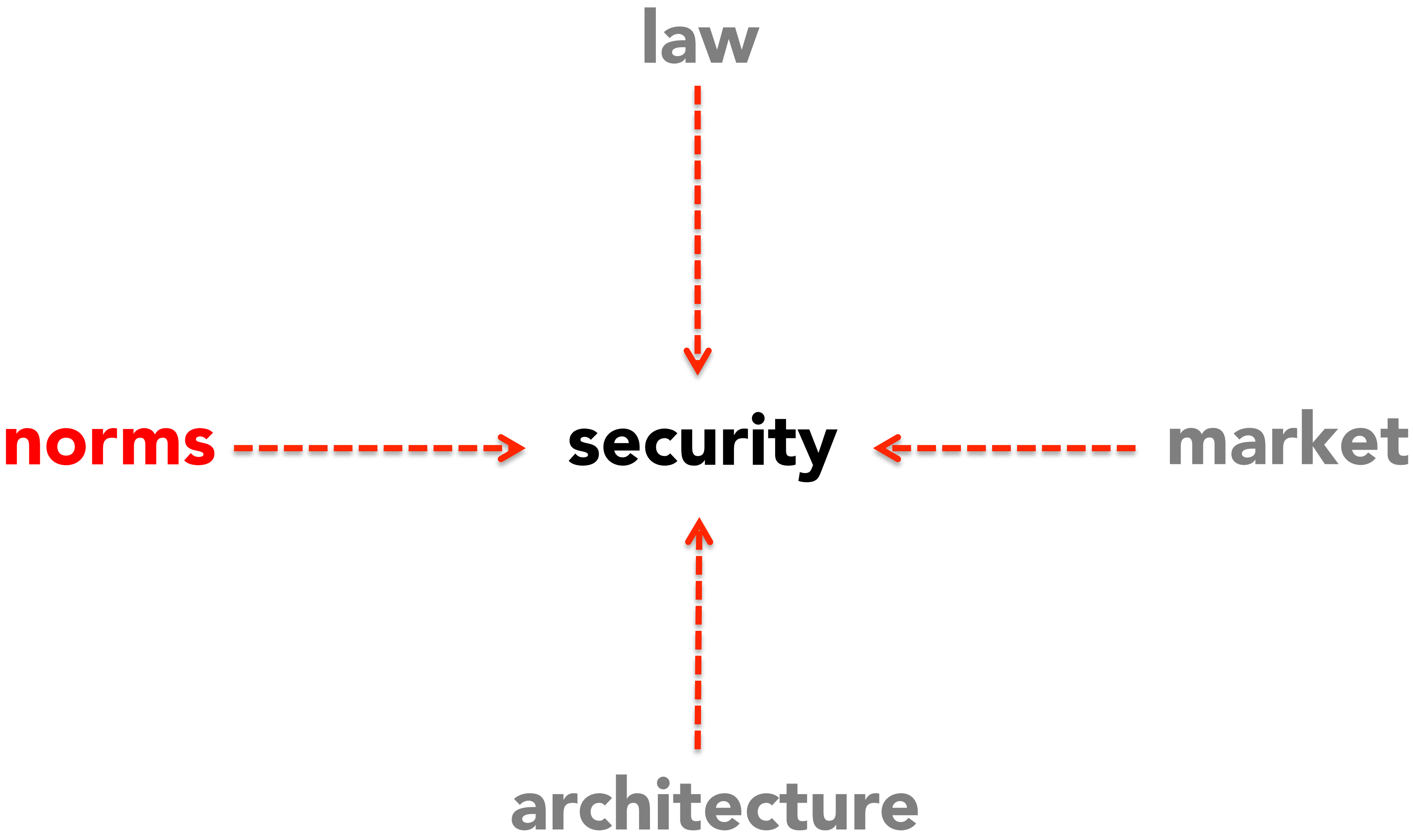
technical critiques of proposals to weaken security

MISSION CRITICAL

technical critiques of proposals to weaken security concrete input on the negative effects of security-related export restrictions

MISSION
CRITICAL

concrete input on the negative effects of security-related export restrictions



law

norms

security

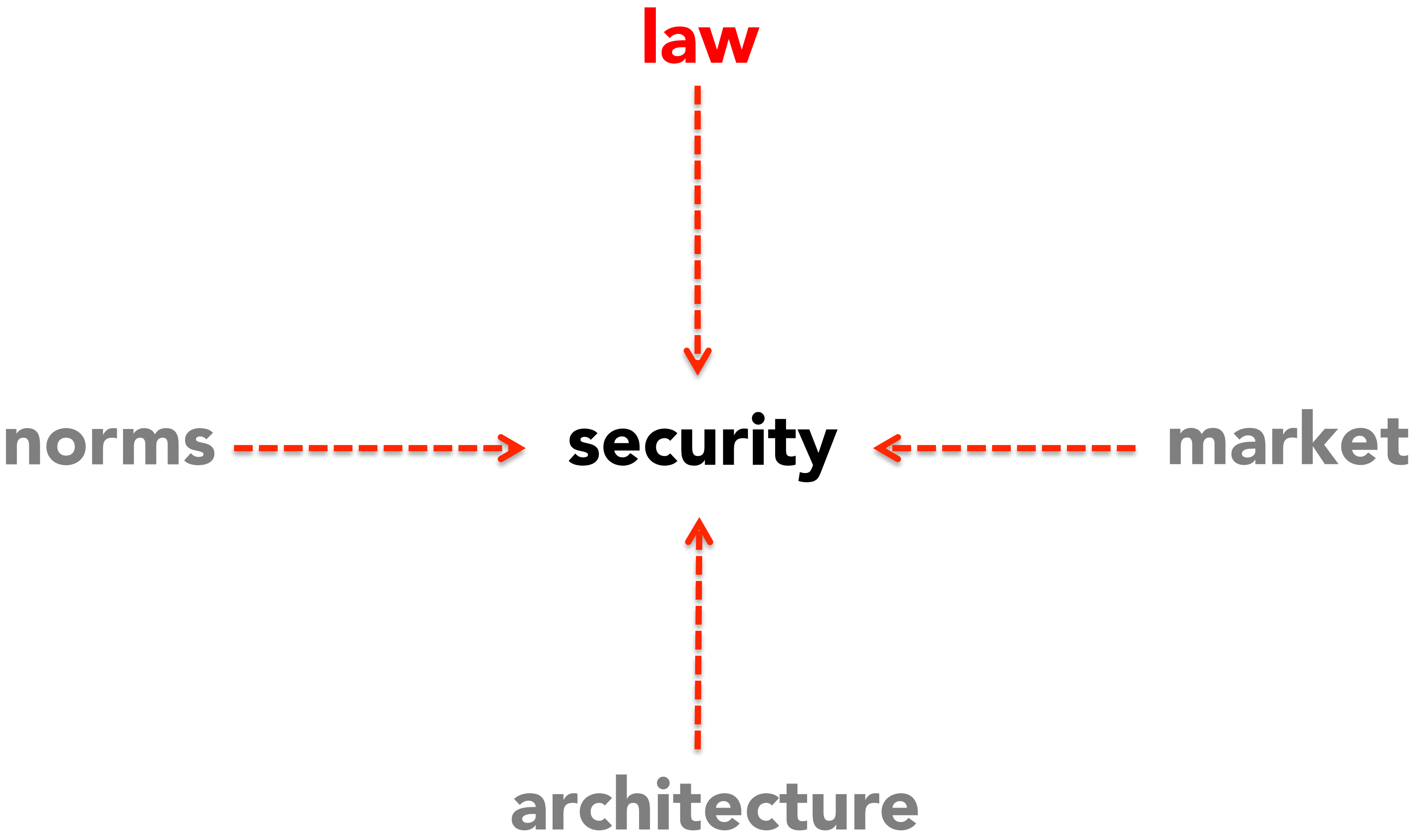
market

architecture

Lawrence Lessig, Code and Other Laws of Cyberspace

widespread &
easy to use by default

expected by consumers



law

norms

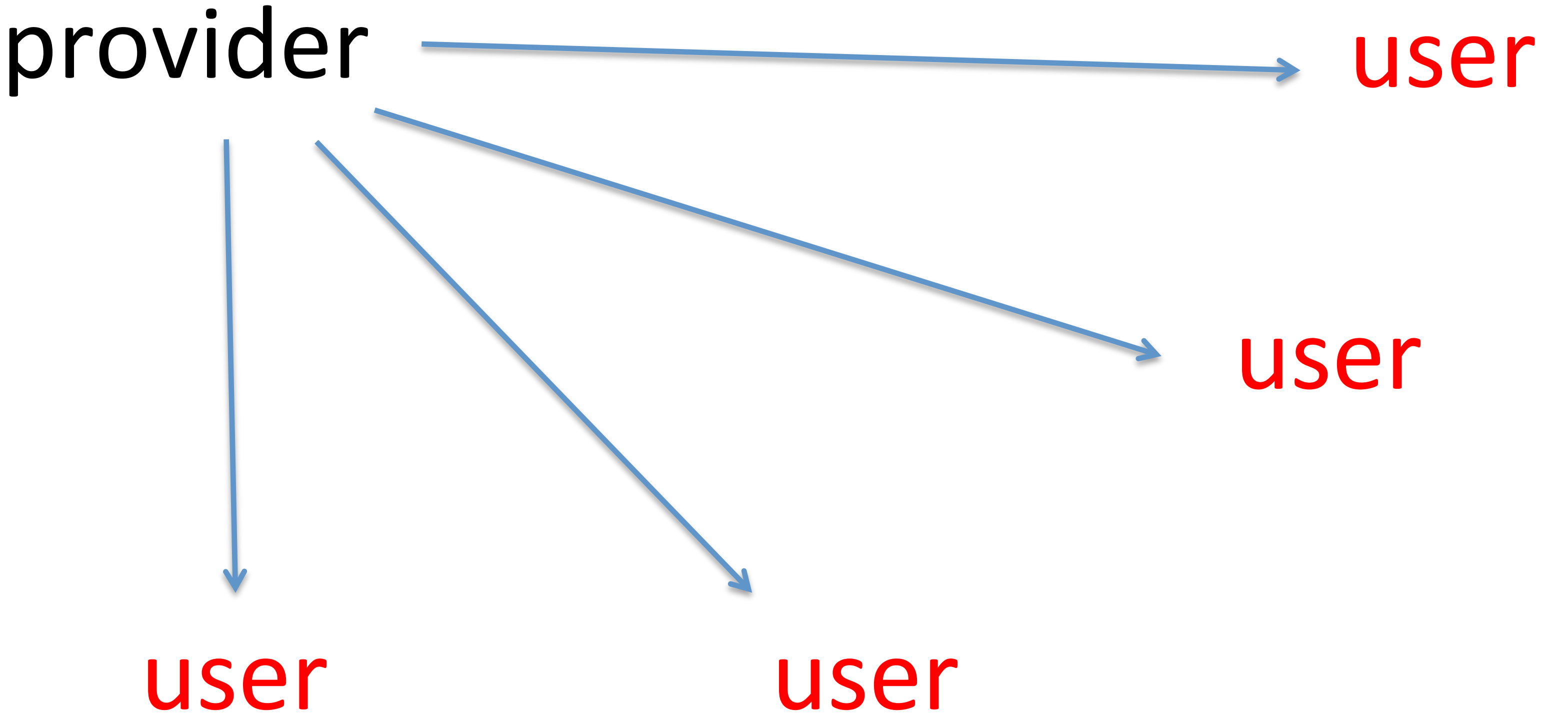
security

market

architecture

Lawrence Lessig, Code and Other Laws of Cyberspace

shift in legal pressure points



provider

user

user

user

user

a fight over whether to design backdoors in products and online services…

a fight over whether to design backdoors in products and online services…

…in both legislatures and the courts

potential legal challenges to
new export controls,
when finalized

what now?

discuss.