

The Second Crypto War: What's Different Now

Susan Landau

Fletcher School of Law & Diplomacy and School of Engineering

Tufts University



Apple Fights Order to Unlock San Bernardino Gunman's iPhone

By ERIC LICHTBLAU and KATIE BENNER FEB. 17, 2016



Timothy D. Cook, the chief executive of Apple, released a letter to customers several hours after a California judge ordered the company to unlock an iPhone used by one of the shooters in a recent attack that killed 14 people in San Bernardino. *Jeff Chiu/Associated Press*

The Apple-F.B.I. Ca

With Finality, F.B.I. Opts
Unlocking Method

■ F.B.I. Director Sugges
Hacking Topped \$1.3 Mill

■ F.B.I. Says It Needs H
With Tech Companies

F.B.I. Used Hacking Softw
iPhone Fight

F.B.I. Lawyer Won't Say i
iPhone Is Useful

[See More »](#)

RECENT COMMENTS

Chevy February 18, 2016
Am I missing something? Wi
privacy of a couple of terrori
of...

U.S. Says It May Not Need Apple's Help to Unlock iPhone

By KATIE BENNER and MATT APUZZO MARCH 21, 2016



RIVERSIDE, Calif. — The Justice Department said on Monday that it might no longer need Apple's assistance in opening an iPhone used by a gunman in the San Bernardino, Calif., rampage last year.

The disclosure led a judge to postpone a court hearing over the issue and temporarily sidesteps what has become a bitter clash with the world's most valuable publicly traded company.

In a new court filing, the government said an outside party had demonstrated a way for the F.B.I. to possibly unlock the phone used by the gunman, Syed Rizwan Farook. The hearing in the contentious case — Apple has loudly opposed opening the iPhone, citing privacy concerns and igniting

The Apple-F.B.I. Case

With Finality, F.B.I. Opts Not to Unlocking Method

■◀ F.B.I. Director Suggests Bill Hacking Topped \$1.3 Million

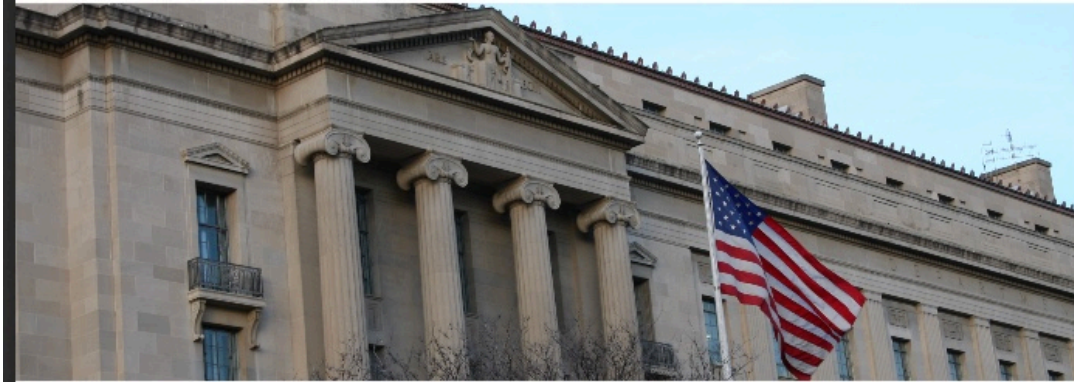
■◀ F.B.I. Says It Needs Hackers With Tech Companies

F.B.I. Used Hacking Software D iPhone Fight



Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



**A Special Inquiry Regarding the
Accuracy of FBI Statements
Concerning its Capabilities to
Exploit an iPhone Seized During
the San Bernardino Terror Attack
Investigation**







The Two Crypto Wars

- 1970s-2000: First Crypto Wars.

The Two Crypto Wars

- 1970s-2000: First Crypto Wars.
 - 1970s: Publication.
 - 1980s: Crypto Standards.
 - 1990s: Export Controls.

The Two Crypto Wars

- 1970s-2000: First Crypto Wars.
- 2000-present: “Going Dark.”

The Two Crypto Wars

- 1970s-2000: First Crypto Wars.
- 2000-present: “Going Dark.”
 - 2010: Going Dark is about not being able to understand communications (end-to-end crypto).

The Two Crypto Wars

- 1970s-2000: First Crypto Wars.
- 2000-present: “Going Dark.”
 - 2010: Going Dark is about not being able to understand communications (end-to-end crypto).
 - 2015: Going Dark is also about locked phones.

What People Say about Encryption and Backdoors

What People Say about Encryption and Backdoors

- “I think that it’s a mistake to require companies that are making hardware and software to build a duplicate key or a back door even if you hedge it with the notion that there’s going to be a court order.”
Michael Chertoff, former DHS Secretary, July 2015, *The Atlantic*.

What People Say about Encryption and Backdoors

- “I think that it’s a mistake to require companies that are making hardware and software to build a duplicate key or a back door even if you hedge it with the notion that there’s going to be a court order.”
Michael Chertoff, former DHS Secretary, July 2015, *The Atlantic*.
- “American security is better served with unbreakable end-to-end encryption than it would be served with one or another front door, backdoor, side door, however you want to describe it.” General **Michael Hayden, former NSA Director**, February 2016, *Business Insider*.

What People Say about Encryption and Backdoors

- “I’m not personally one of those who thinks we should weaken encryption because I think there is a parallel issue, which is cybersecurity more broadly ... It’s very important that we should be seen and be a country in which people can operate securely – that’s important for our commercial interests as well as our security interests, so encryption in that context is very positive.” Lord **Jonathan Evans, ex-head MI5**, August 2017, *The Guardian*.

The Two Crypto Wars

- 1970s-2000: First Crypto Wars.
- 2000-present: “Going Dark.”
 - 2010: Going Dark is about not being able to understand communications (end-to-end crypto).
 - 2015: Going Dark is also about locked phones.

Why lock phones?

- Theft of phones.
- Theft of data.

Why lock phones?

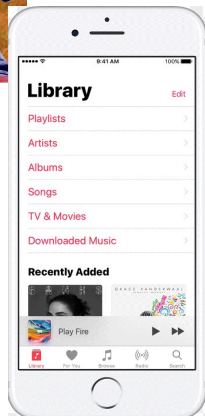
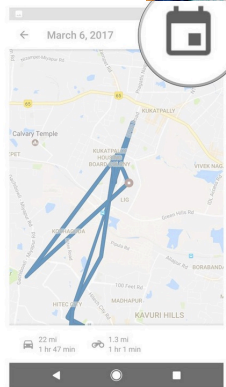
- Theft of phones: Activation Lock.
Find My iPhone.
- Theft of data.

Why lock phones?

- Theft of phones: Activation Lock.
Find My iPhone.
- Theft of data: protection through encryption;
 - the key entangled PIN and device key.

Privacy

Privacy



B

Steve Bellovin

Matt Blaze

Dan Boneh

Bono

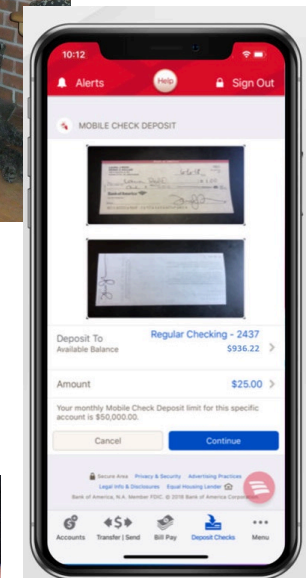
C

A
B
C
D
E
F
G
H
I
J
K
L
M
N

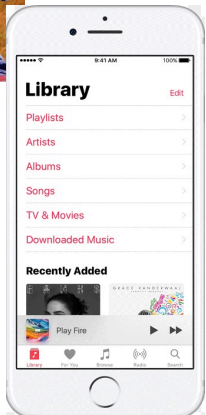
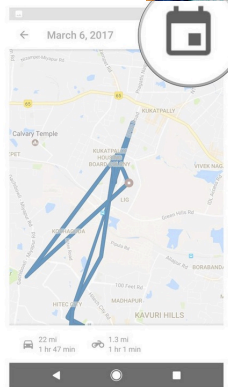
How did your project come out?

Are you finally finished working?

Yes!



Security



Yes!

B

Steve Bellovin

Matt Blaze

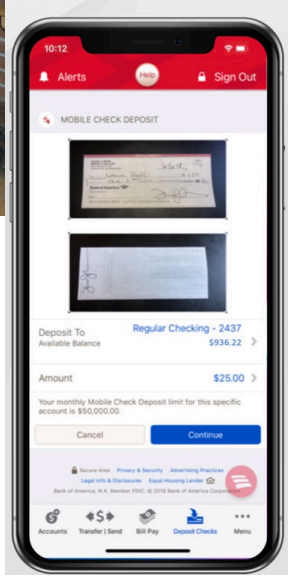
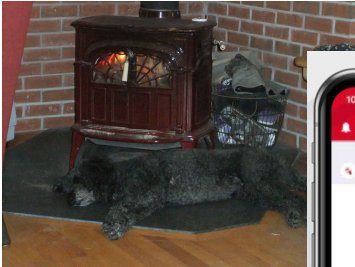
Dan Boneh

Bono

C

A
B
C
D
E
F
G
H
I
J
K
L
M
N

How did your project come out?
Are you finally finished working?



Why lock phones?



Why lock phones?



Why lock phones?

THE BALTIMORE SUN

12 WEEKS FREE Start Trial


SUNDAY NOV. 12, 2017

BREAKING SPORTS MARYLAND BUSINESS OPINION OBITS NEWSPAPER ADVERTISING

ADVERTISEMENT

Lifestyle / Baltimore Insider

Black Lives Matter activist DeRay Mckesson's Twitter hacked Friday morning



Today's Mortgage Rate
3.04%
APR 15 Year Fixed

Select Loan Amount
\$225,000

data from ads.revjet.com... ist and former Baltimore mayoral candidate DeRay Mckesson's Twitter was hacked this morning. (Patrick

THE NEW YORK TIMES

SECTIONS HOME SEARCH

Did Jeff Bewkes Help Time Warner's Cause in Court?: DealBook Briefing

Comcast Bid 16% More Than Disney for 21st Century Fox, Filing Shows


Key Dates to Watch in China-U.S. Trade Dispute: DealBook Briefing

Total, With Energy Industry in Flux, Makes \$1.7 Billion Bet on a Utility

DealBook / Business & Policy

Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency

By NATHANIEL POPPER AUG. 21, 2017



RECENT COMMENTS

Chris August 25, 2017
Welcome to the happy, friendly, "we're all more co ever" world of sunshine and lollipops.Ironic that the digital...

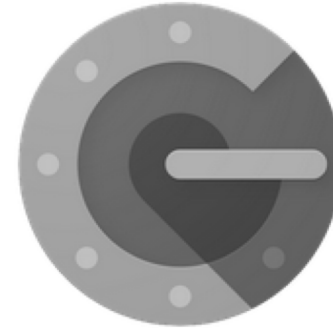
janet August 23, 2017
Yet another reason why I refuse to use my cell on r Of course, I have a stupidphone and no financial at it's not as...

Trista August 23, 2017
I think as technology gets more sophisticated, a pe will be able to be used as an identifier. It would be impossible to...

SEE ALL COMMENTS

Hackers have discovered that one of the most central elements of online security — the mobile phone number — is also one of the easiest to steal. Kevin Hagen for The New York Times

Why lock phones?



So how do you do investigations in the
Digital Age?

News Front Page



- Africa
- Americas
- Asia-Pacific
- Europe
- Middle East
- South Asia

- UK**
- England
- Northern Ireland
- Scotland
- Wales
- UK Politics
- Education
- Magazine

- Business**
- Health
- Science & Environment
- Technology
- Entertainment
- Also in the news

Last Updated: Saturday, 30 July 2005, 01:08 GMT 02:08 UK

E-mail this to a friend

Printable version

Failed bomb attacks: What we know

The latest details of the attempts to detonate bombs on three London Tube trains and a bus on Thursday 21 July, following a series of arrests on Friday.

BOMB SUSPECTS

London Underground lines

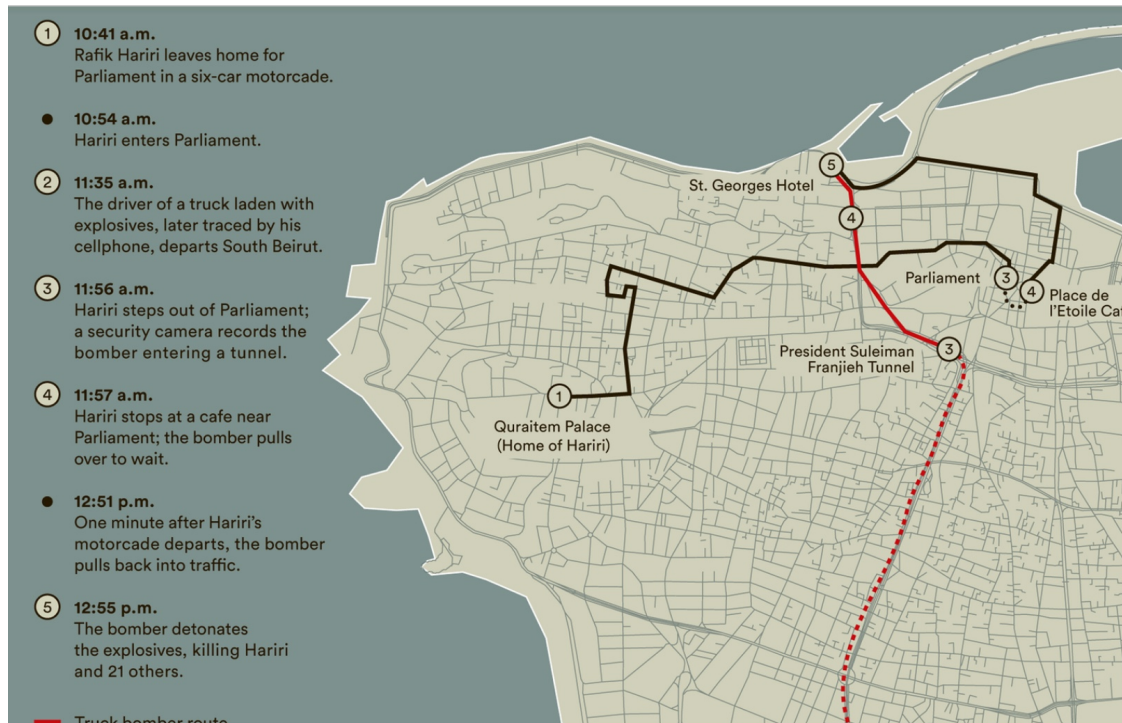
- Hammersmith & City
- Victoria
- Northern
- ⊖ Station

All journeys started between 12:20 and 12:25 BST. Times approx.

CBCnews



A closed-circuit TV image released by the Metropolitan Police shows the four London bombers arriving at Luton railway station at 7:21 a.m. local time on Thursday, July 7, 2005. The image shows, from left to right, Hasib Hussain, Jermaine Lindsay (dark cap), Mohammed Sidique Khan (light cap), and Shahzad Tanweer. (AP Photo/Metropolitan Police)



Map from "The Hezbollah Connection," New York Times Magazine.

- In 2007, the Security and Exchange Commission gets a tip about the Galleon Group.

- By 2011, 35 people are convicted; Rajaratnam gets an 11-year sentence.

- An IM that said, “do not buy plcm till i het guidance.”

How would law enforcement investigate?

Probe ID	Call ID	Orig	Calling	Called	Start	Released	Duration	Rel Code
ATTCARD1	111116111506-1	New York(#2:0)	3016041111	3019241111	11/16/2011 11:15:24	11/16/2011 11:16:58	00:01:34	Normal
ATTCARD1	111116111506-3	New York(#2:2)	3016243333	3019243333	11/16/2011 11:15:24	11/16/2011 11:16:05	00:00:41	Normal
ATTCARD1	111116111506-24	New York(#2:22)	3017242222	3019242222	11/16/2011 11:15:29	11/16/2011 11:16:11	00:00:42	Normal
ATTCARD1	111116111506-2	New York(#2:1)	3016042222	3019242222	11/16/2011 11:15:24	11/16/2011 11:16:07	00:00:43	Normal
ATTCARD1	111116111506-21	New York(#2:20)	3012242220	3019242220	11/16/2011 11:15:25	11/16/2011 11:16:06	00:00:41	Normal
ATTCARD1	111116111506-19	New York(#2:18)	3017242218	3019242218	11/16/2011 11:15:25	11/16/2011 11:16:08	00:00:43	Normal
ATTCARD1	111116111506-18	New York(#2:17)	3015242217	3019242217	11/16/2011 11:15:25	11/16/2011 11:16:08	00:00:43	Normal
ATTCARD1	111116111506-17	New York(#2:16)	3016242216	3019242216	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-16	New York(#2:15)	3016242215	3019242215	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-15	New York(#2:14)	3016242214	3019242214	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-14	New York(#2:13)	3016242213	3019242213	11/16/2011 11:15:24	11/16/2011 11:16:07	00:00:43	Normal
ATTCARD1	111116111506-13	New York(#2:12)	3016242212	3019242212	11/16/2011 11:15:24	11/16/2011 11:16:07	00:00:43	Normal
ATTCARD1	111116111506-12	New York(#2:11)	3016241011	3019241011	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-11	New York(#2:10)	3016241010	3019241010	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-10	New York(#2:9)	3019242289	3017242239	11/16/2011 11:15:24	11/16/2011 11:16:06	00:00:42	Normal
ATTCARD1	111116111506-9	New York(#2:8)	3019242288	301724				
ATTCARD1	111116111506-8	New York(#2:7)	3019242237	301624				
ATTCARD1	111116111506-7	New York(#2:6)	3019242236	301624				
ATTCARD1	111116111506-6	New York(#2:5)	3019242235	301624				
ATTCARD1	111116111506-5	New York(#2:4)	3019242234	301624				
ATTCARD1	111116111506-4	New York(#2:3)	3019242233	301624				
ATTCARD1	111116111506-22	New York(#2:21)	3019242221	301624				
ATTCARD1	111116111506-20	New York(#2:19)	3014242219	301224				

F.B.I. Used Hacking Software Decade Before iPhone Fight

By MATT APUZZO APRIL 13, 2016



Director Comey photo from New York Times



How would law enforcement investigate?



Investigations in the Digital Age

- Investigations in the Digital Age:

Investigations in the Digital Age

- Investigations in the Digital Age:
 - A high percentage of crimes have a digital component.
 - Far more data is concentrated at service providers.
 - The laws on collection and surveillance largely predate the Digital Age.

Investigations in the Digital Age



From: CSIS, *Low-Hanging Fruit*, 2018.

How should law enforcement investigate?

- Retool to become an investigative agency of the Digital Age.
- Better capability sharing between federal and state and local.
- More funding.

How should law enforcement investigate?

- Retool to become an investigative agency of the Digital Age.
 - Assume all investigations have a digital component.
 - Enhance outreach to industry.
- Better capability sharing between federal and state and local.
- More funding.

How should law enforcement investigate?

- Retool to become an investigative agency of the Digital Age.
 - Assume all investigations have a digital component.
 - Enhance outreach to industry.
- Better capability sharing between federal and state and local.
 - Sharing and access to specialized services.
- More funding.

How should law enforcement investigate?

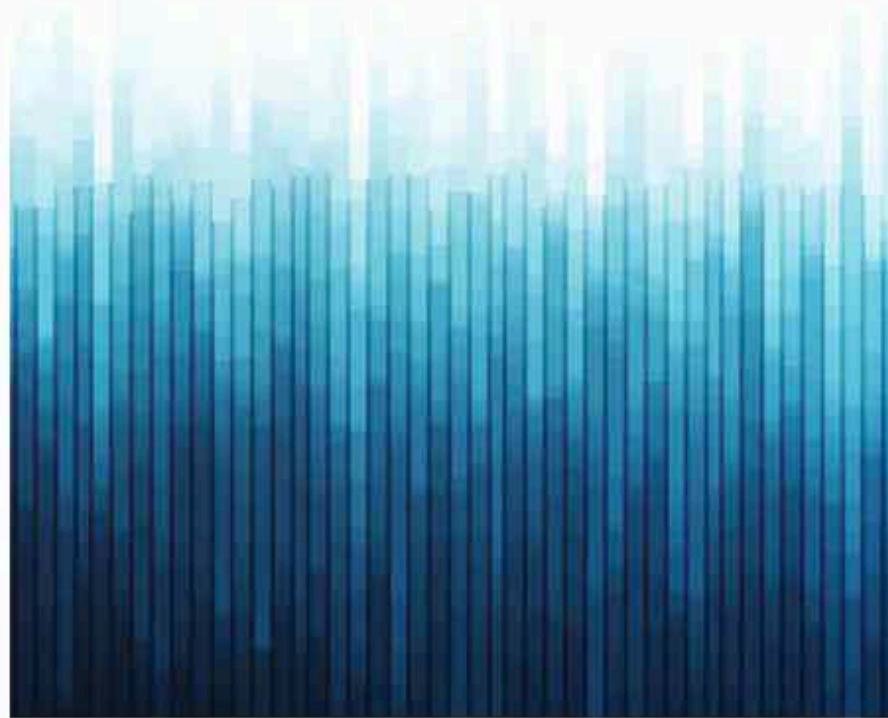
- Retool to become an investigative agency of the Digital Age.
 - Assume all investigations have a digital component.
 - Enhance outreach to industry.
- Better capability sharing between federal and state and local.
 - Sharing and access to specialized services.
- More funding.

Need to decide investigative priorities.

CONSENSUS STUDY REPORT

Decrypting the
ENCRYPTION DEBATE

A Framework for Decision Makers



Decrypting the Encryption Debate: limitations

- Incomplete data on impact on law enforcement:
 - Doesn't actually address impact of encryption on investigations.
- Limited ability to measure additional security risks.

Decrypting the Encryption Debate

Charge

- Study tradeoffs associated with mechanisms for authorized government agencies access to plaintext of encrypted information.

Approach

- Explore legal and technical options available to governments.
- Provide a framework—a set of questions—to ask re any path forward.

Decrypting the Encryption Debate

Charge

- Study tradeoffs associated with mechanisms for authorized government access to plaintext of encrypted information.

Approach

- Explore legal and technical options available to governments.
- Provide a framework—a set of questions—to ask re any path forward.

No recommendations.

Decrypting the Encryption Debate: Framework Questions

1. Is proposed approach **effective, work at scale, timely** and **reliable**?
2. How will it affect **security of data and device**, as well **cybersecurity** broadly?
3. How will affect **privacy and civil liberties** of **targeted and untargeted** individuals?
4. How will proposed approach affect **commerce, economic competitiveness, and innovation**?

Decrypting the Encryption Debate: Framework Questions

5. What are **financial costs** and **who bears** them?
6. To what extent is **approach consistent** with **current laws** and other **government priorities**?
7. How does **international context** affect approach?
8. Will approach be subject to **effective evaluation and oversight**?

Decrypting the Encryption Debate: Fundamental Tradeoff

Adding Exceptional Access capability to encryption necessarily weakens security to some degree; its lack necessarily hampers investigations.

Decrypting the Encryption Debate: Fundamental Tradeoff

Adding Exceptional Access capability to encryption necessarily weakens security to some degree; its lack necessarily hampers investigations:

- How much security is reduced? Is resulting level of security acceptable?
 - This depends on specific technical and operational details of the mechanism.

Decrypting the Encryption Debate: Fundamental Tradeoff

Adding Exceptional Access capability to encryption necessarily weakens security to some degree; its lack necessarily hampers investigations:

- How much security is reduced? Is resulting level of security acceptable?
 - This depends on specific technical and operational details of the mechanism.
- Cost to society when an investigation is hindered or thwarted.

Decrypting the Encryption Debate:

- Some computer scientists have reacted with concern to renewed proposals to regulate the use of encryption, citing security risks.
- Three technical approaches were presented to the committee that would minimize these risks. These were not fully fleshed out, tested, or deployed.



Decrypting the Encryption Debate

- Ozzie CLEAR proposal:
 - Only for locked devices.
 - Model is for decryption key to be “wrapped” by manufacturer’s key.
 - Device bricks upon being unlocked.
 - CLEAR “proposal” is not for a system; it shows only how to retrieve key securely.

Decrypting the Encryption Debate

- Ozzie CLEAR proposal:
 - Only for locked devices.
 - Model is for decryption key to be “wrapped” by manufacturer’s key.
 - Device bricks upon being unlocked.
 - CLEAR “proposal” is not for a system; it shows only how to retrieve key securely.

This is a systems problem.

Decrypting the Encryption Debate

- Ozzie CLEAR proposal:
 - Only for locked devices.
 - Model is for decryption key to be “wrapped” by manufacturer’s key.
 - Device bricks upon being unlocked.
 - CLEAR “proposal” is not for a system; it shows only how to retrieve key securely.
 - Technique subject to spoofing—attack due to Eran Tromer.
 - Technique not resistant to jail breaking.
 - Can’t answer framework questions: insufficient detail.
 - Moving target.

Steve Bellovin, Matt Blaze, Dan Boneh, Susan Landau, Ron Rivest

Decrypting the Encryption Debate

Decrypting the Encryption Debate

“If smartphones are used to provide authentication codes in a multifactor authentication scheme, a requirement for exceptional access to unlock smartphones adds some degree of risk that the authentication codes could be obtained from a lost or stolen phone.”

Why Encourage Cryptography's Use?



**Background to "Assessing Russian Activities and Intentions
in Recent US Elections": The Analytic Process and Cyber
Incident Attribution**

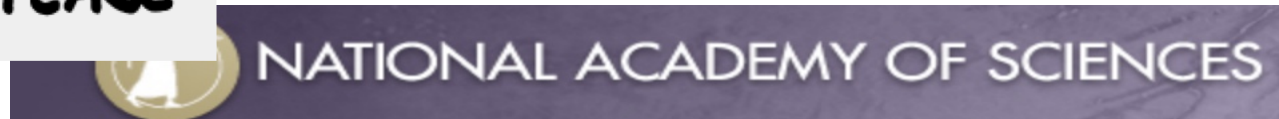
Why Encourage Cryptography's Use?

We assess Russian intelligence services collected against the US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies.

Role of Civil Society



GREENPEACE



SPLC
Southern Poverty
Law Center

In a nutshell

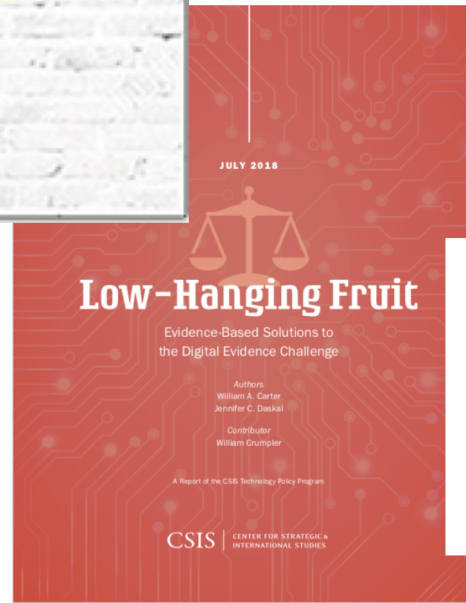
The Going Dark debate is **not** about **privacy versus security**.

In a nutshell

The Going Dark debate is really about **efficiency of law-enforcement investigations versus personal, business, and national security.**

In a nutshell

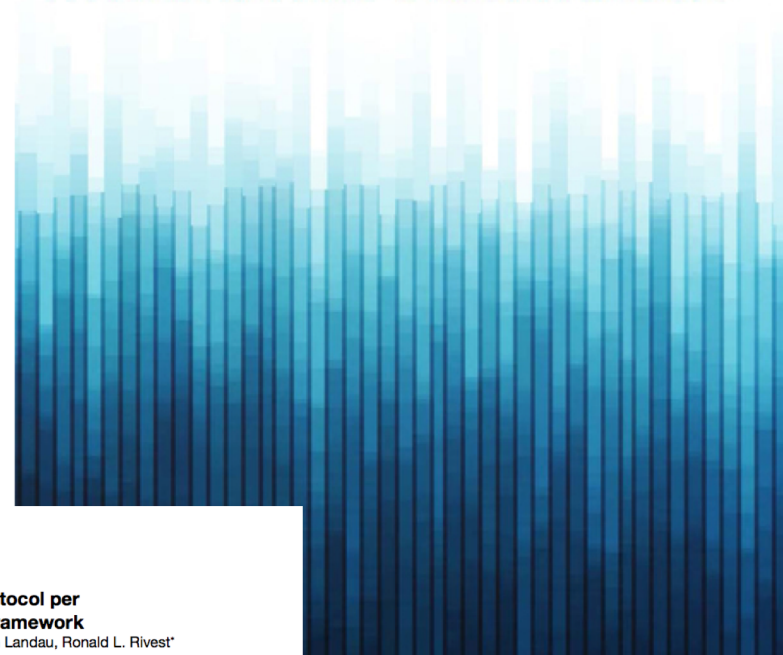
This Going Dark debate is about **security versus security**.



CONSENSUS STUDY REPORT

Decrypting the ENCRYPTION DEBATE

A Framework for Decision Makers



Analysis of the CLEAR Protocol per the National Academies' Framework

Steven M. Bellovin, Matt Blaze, Dan Boneh, Susan Landau, Ronald L. Rivest*
CUCS-003-18
May 10, 2018

Abstract: The debate over “exceptional access”—the government’s ability to read encrypted data—has been going on for many years and shows no signs of resolution any time soon. On the one hand, some people claim it can be accomplished safely; others dispute that. In an attempt to make progress, a National Academies study committee propounded a framework to use when analyzing proposed solutions. We apply that framework to the CLEAR protocol and show the limitations of the design.