Compelled Decryption

State of the Art Doctrinal Perversions

by Ladar Levison
Owner and Operator, Lavabit LLC

Version 1.0

July 8th 2016

DEF CON 24 PRESENTATION PREVIEW

PLEASE NOTE

THESE SLIDES ARE PRELIMINARY
EXPECT ALTERATIONS

School of Hard Knocks

Presents

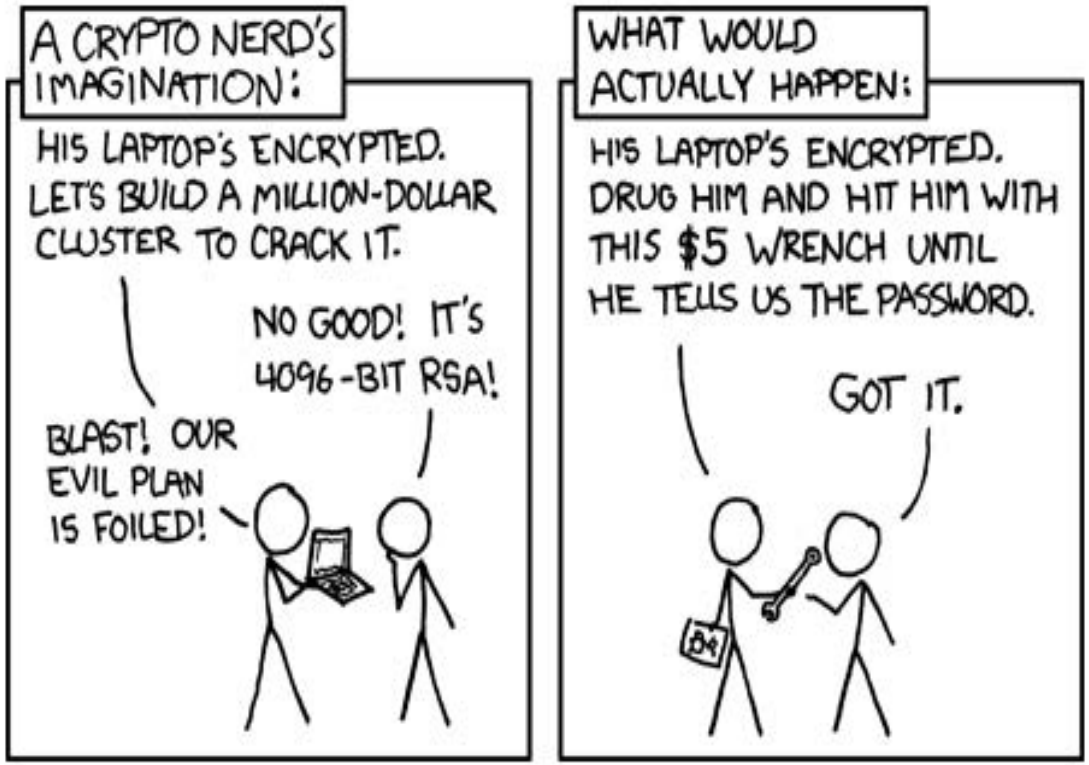
Ladar Levison

this

Master of Misfortune

on the 2nd day of August in the year 2013




A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
xkcd



within the mainstream, but this is a provider that specifically was started in order to have to protect privacy interests more than the average Internet service provider.

THE COURT: I can understand why the system was set up, but I think the government is -- government's clearly entitled to the information that they're seeking, and just because you-all have set up a system that makes that difficult, that doesn't in any way lessen the government's right to receive that information just as they would from any telephone company or any other e-mail source that could provide it easily. Whether it's -- in other words, the difficulty or the ease in obtaining the information doesn't have anything to do with whether or not the government's lawfully entitled to the information.

devised by Apple. As the Supreme Court held, the Act supplies a basis for a court to order a third-party corporation to assist in gathering evidence. As the Ninth Circuit held, that precedent permits a court to order a corporation to program a computer, even if the corporation objects that doing so will cost it money, divert its technicians, and annoy its customers. That controlling precedent and the All Writs Act—not Apple's technological fiat—should determine whether Farook's iPhone will be searched.

Apple and its *amici* try to alarm this Court with issues of network security, encryption, back doors, and privacy, invoking larger debates before Congress and in the news media. That is a diversion. Apple desperately wants—desperately *needs*—this case not to be "about one isolated iPhone." But there is probable cause to believe there is evidence of a terrorist attack on that phone, and our legal system gives this Court the authority to see that it can be searched pursuant to a lawful warrant. And under the compelling circumstances here, the Court should exercise that authority, even if Apple would rather its products be warrant-proof.

This case—like the three-factor Supreme Court test on which it must be decided—is about specific facts, not broad generalities. Here, Apple deliberately raised technological barriers that now stand between a lawful warrant and an iPhone containing evidence related to the terrorist mass murder of 14 Americans. Apple alone can remove those barriers so that the FBI can search the phone, and it can do so without undue burden. Under those *specific* circumstances, Apple can be compelled to give aid. That is not lawless tyranny. Rather, it is ordered liberty vindicating the rule of law. This


KNOWING
IS HALF THE BATTLE

First Party

vs

Third Party

The Washington Post

National Security

Justice Dept. grants immunity to staffer who set up Clinton email server



The Justice Department granted immunity to the former State Department staffer who set up Hillary Clinton's private email server at her home. Here's what the FBI is looking to investigate and what it means for the Democratic presidential front-runner. (Victoria Walker/The Washington Post)

By Adam Goldman March 2

The Justice Department has granted immunity to a former State Department staffer, who worked on Hillary Clinton's private email server, as part of a criminal investigation into the possible mishandling of classified information, according to a senior law enforcement official.

The official said the FBI had secured the cooperation of Bryan Pagliano, who worked on Clinton's 2008 presidential campaign before setting up the server in her New York home in 2009.

MUCKROCK



February 3, 2014

DEA teaches agents to recreate evidence chains to hide methods

Trainers justify parallel construction on national security and PR grounds: "Americans don't like it"

Written by Shawn Musgrave

Edited by Michael Morisy

Drug Enforcement Administration training documents released to MuckRock user C.J. Ciaramella show how the agency constructs two chains of evidence to hide surveillance programs from defense teams, prosecutors, and a public wary of domestic intelligence practices.

In training materials, the department even encourages a willful ignorance by field agents to minimize the risk of making intelligence practices public.


ANOTHER ISP'S FILTERING CONTENT.
THANK GOD FOR CRYPTO.
IT WASN'T THAT LONG AGO THAT RSA WAS ILLEGAL TO EXPORT. CLASSIFIED A MUNITION.
YOU KNOW, I THINK THE CRYPTO COMMUNITY TOOK THE WRONG SIDE IN THAT FIGHT. WE SHOULD'VE LOBBIED TO KEEP IT COUNTED AS WEAPONRY.
WHY?
ONCE THEY GET COMPLACENT, WE BREAK OUT THE SECOND AMENDMENT
...DAMN.
xkcd

Communications Assistance for Law Enforcement Act (aka CALEA)

(2) INFORMATION SERVICES; PRIVATE NETWORKS AND INTERCONNECTION SERVICES AND FACILITIES- The requirements of subsection (a) do not apply to--

(A) information services; or
(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

(3) ENCRYPTION- A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

(c) EMERGENCY OR EXIGENT CIRCUMSTANCES- In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of title 18, United States Code, and section 1805(e) of title 50 of such Code), a carrier at its discretion may comply with subsection (a)(3) by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

(d) MOBILE SERVICE ASSISTANCE REQUIREMENTS- A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-

The Washington Post

National Security

NSA broke privacy rules thousands of times per year, audit finds

By Barton Gellman August 15, 2013

snipped...

In one instance, the NSA decided that it need not report the unintended surveillance of Americans. A notable example in 2008 was the interception of a "large number" of calls placed from Washington when a programming error confused the U.S. area code 202 for 20, the international dialing code for Egypt, according to a "quality assurance" review that was not distributed to the NSA's oversight staff.

snipped...

The Obama administration has provided almost no public information about the NSA's compliance record. In June, after promising to explain the NSA's record in "as transparent a way as we possibly can," Deputy Attorney General James Cole described extensive safeguards and oversight that keep the agency in check. "Every now and then, there may be a mistake," Cole said in congressional testimony.

The NSA audit obtained by The Post, dated May 2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. Most were unintended. Many involved failures of due diligence or violations of standard operating procedure. The most serious incidents included a violation of a court order and unauthorized use of data about more than 3,000 Americans and green-card holders.

PROPUBLICA | Journalism in the Public Interest

Trial and Error: Report Says Prosecutors Rarely Pay Price for Mistakes and Misconduct

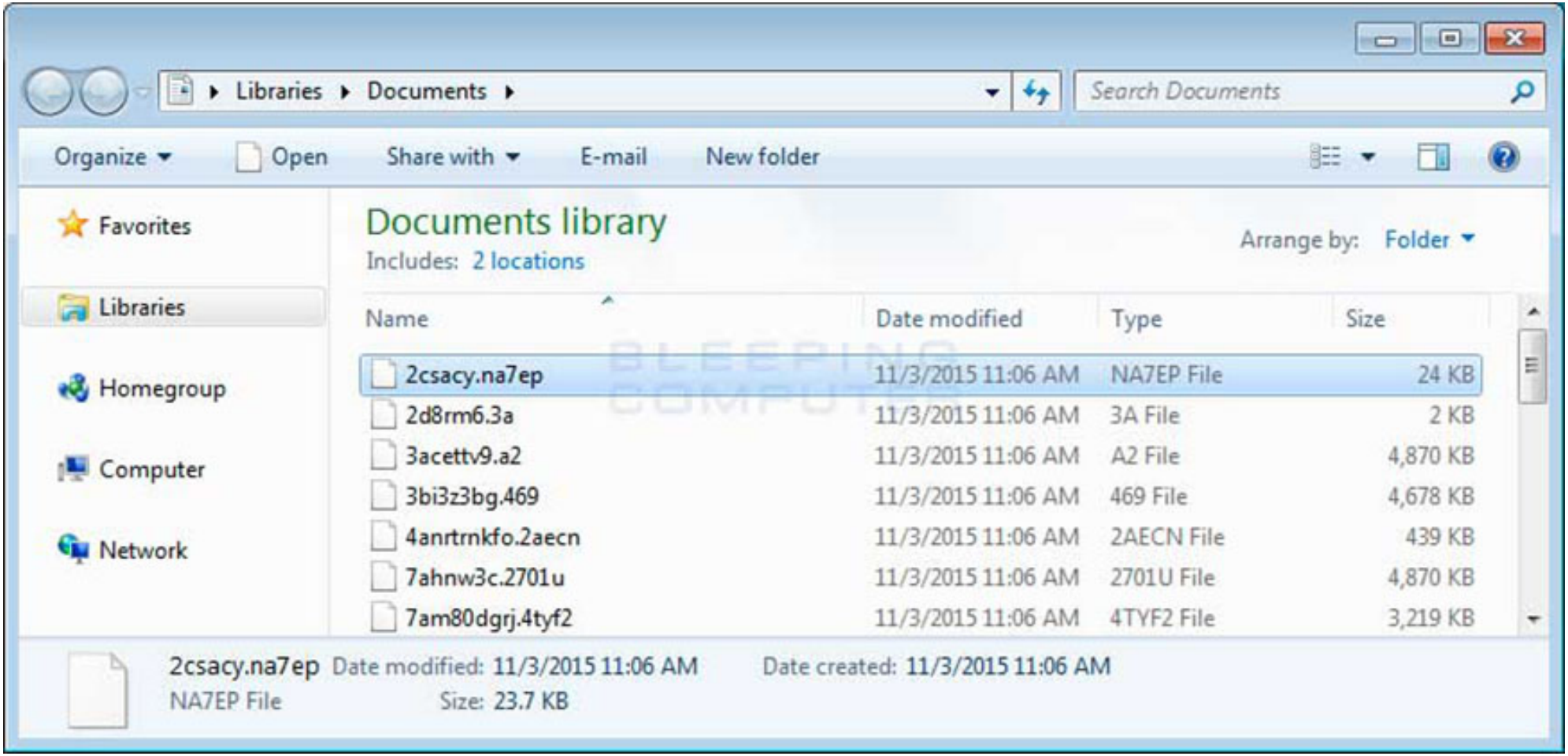
by Joaquin Sapien
ProPublica, March 29, 2016, 8 a.m.



INNOCENCE PROJECT

Prosecutorial Oversight:

A National Dialogue in the Wake of *Connick v. Thompson*


Libraries ▸ Documents ▸
Search Documents
Organize
Open
Share with
E-mail
New folder
Favorites
Libraries
Homegroup
Computer
Network
Documents library
Includes: 2 locations
Arrange by: Folder
Name
Date modified
Type
Size
2csacy.na7ep 11/3/2015 11:06 AM NA7EP File 24 KB
2d8rm6.3a 11/3/2015 11:06 AM 3A File 2 KB
3acettv9.a2 11/3/2015 11:06 AM A2 File 4,870 KB
3bi3z3bg.469 11/3/2015 11:06 AM 469 File 4,678 KB
4anrtrnkfo.2aecn 11/3/2015 11:06 AM 2AECN File 439 KB
7ahnw3c.2701u 11/3/2015 11:06 AM 2701U File 4,870 KB
7am80dgrj.4tyf2 11/3/2015 11:06 AM 4TYF2 File 3,219 KB
2csacy.na7ep Date modified: 11/3/2015 11:06 AM Date created: 11/3/2015 11:06 AM
NA7EP File Size: 23.7 KB

How [redacted] uses Encryption to Protect your Data



Accessing your data

Upon arriving at a [redacted] datacenter, your data is assigned to one or more Storage Pods where it is stored encrypted. Access to your data is secured by your [redacted] account login information (your email address and password). When you provide these credentials, your private key is used to decrypt your data. At this point you can view your file/folder list and request a restore as desired.

New: [redacted] has enabled two-factor authentication. Now a 6-digit code can be sent to your phone during sign-in for an extra layer of security.









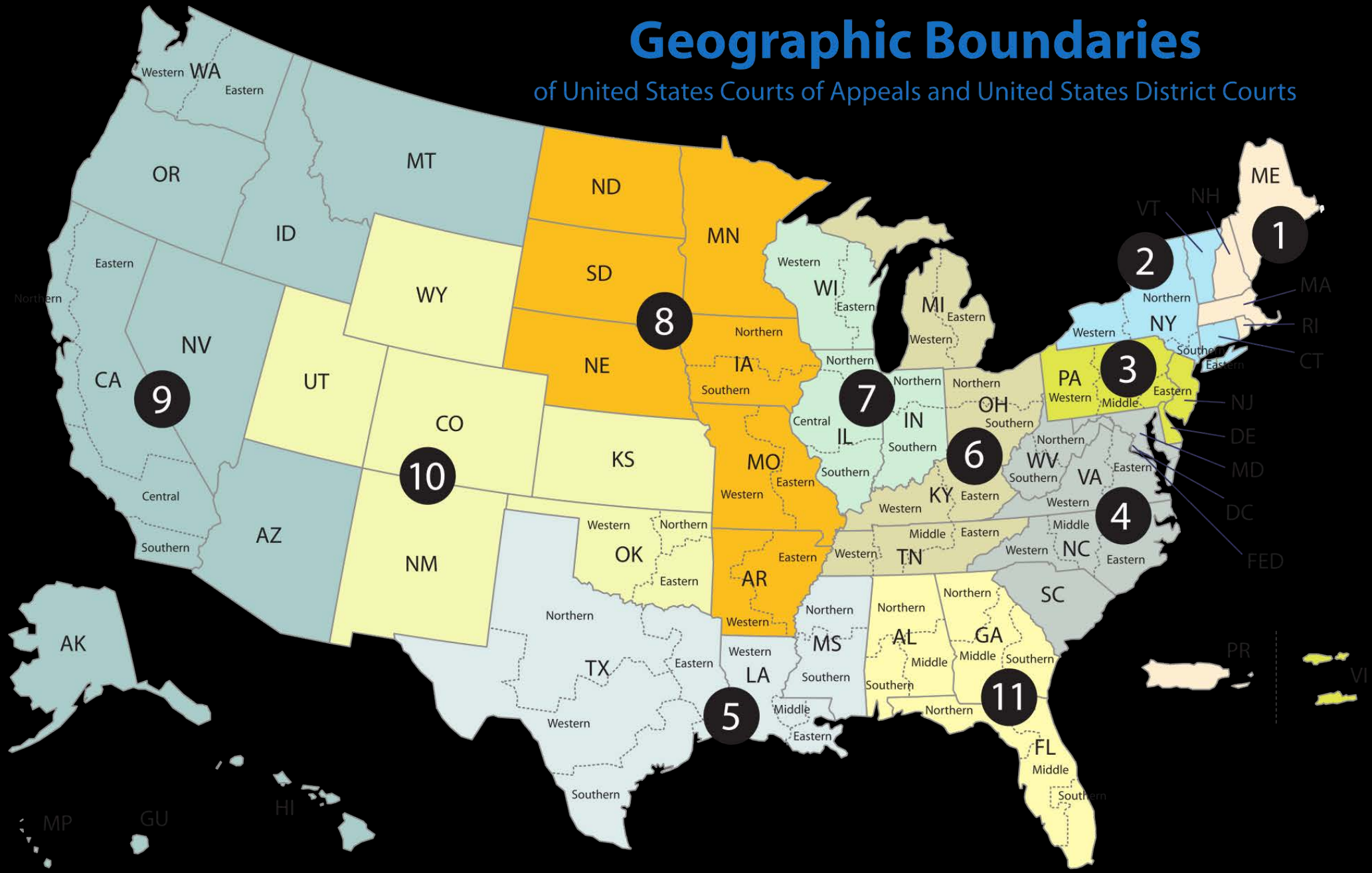


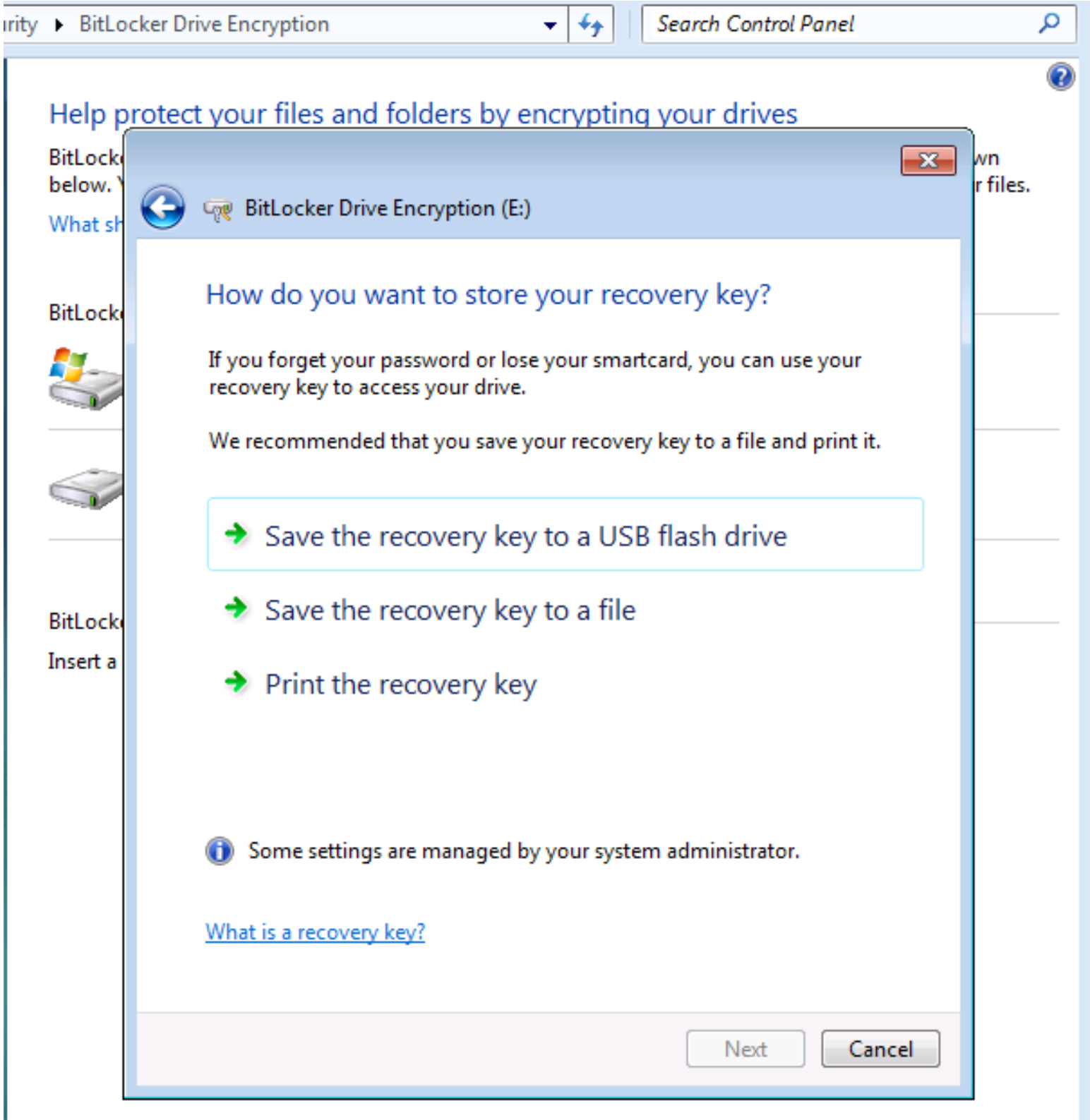

I AM AS RADIANT
AS THE SUN



Geographic Boundaries

of United States Courts of Appeals and United States District Courts




rity ▸ BitLocker Drive Encryption
Search Control Panel
Help protect your files and folders by encrypting your drives
BitLock
below.
What sh
BitLock
BitLock
Insert a
wn
r files.
BitLocker Drive Encryption (E:)
How do you want to store your recovery key?
If you forget your password or lose your smartcard, you can use your recovery key to access your drive.
We recommended that you save your recovery key to a file and print it.
Save the recovery key to a USB flash drive
Save the recovery key to a file
Print the recovery key
Some settings are managed by your system administrator.
What is a recovery key?
Next
Cancel

Recovery setup

Using Group Policy, an IT administrator can choose which recovery methods to require, deny, or make optional for users who enable BitLocker. The recovery password can be stored in AD DS, and the administrator can make this option mandatory, prohibited, or optional for each user of the computer. Additionally, the recovery data can be stored on a USB flash drive.

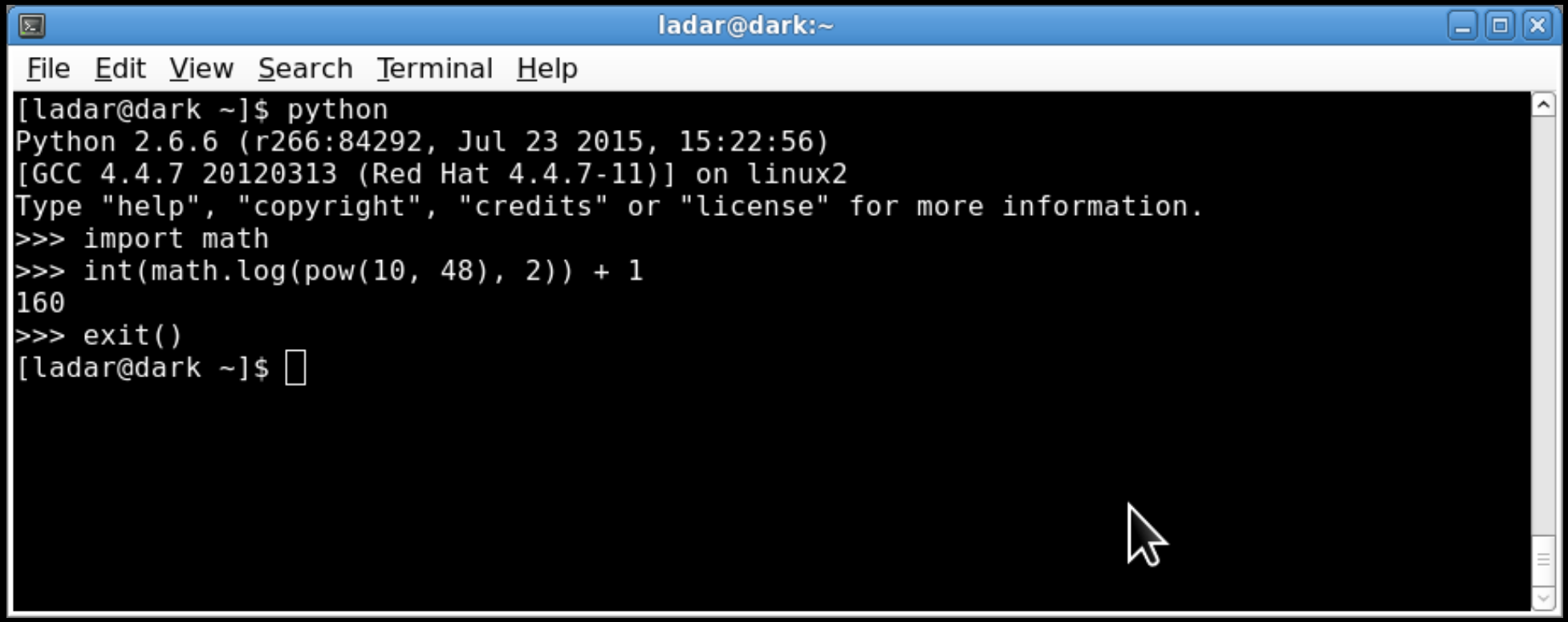
Recovery password

The recovery password is a 48-digit, randomly generated number that can be created during BitLocker setup. If the computer enters recovery mode, the user will be prompted to type this password by using the function keys (F0 through F9). The recovery password can be managed and copied after BitLocker is enabled. Using the **Manage BitLocker** page in the **BitLocker Drive Encryption** item in Control Panel, the recovery password can be printed or saved to a file for future use.

A domain administrator can configure Group Policy to generate recovery passwords automatically and back them up to AD DS as soon as BitLocker is enabled. The domain administrator can also choose to prevent BitLocker from encrypting a drive unless the computer is connected to the network and AD DS backup of the recovery password is successful.

Recovery key

The recovery key can be created and saved to a USB flash drive during BitLocker setup; it can also be managed and copied after BitLocker is enabled. If the computer enters recovery mode, the user will be prompted to insert the recovery key into the computer.


ladar@dark:~
File Edit View Search Terminal Help
[ladar@dark ~]$ python
Python 2.6.6 (r266:84292, Jul 23 2015, 15:22:56)
[GCC 4.4.7 20120313 (Red Hat 4.4.7-11)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import math
>>> int(math.log(pow(10, 48), 2)) + 1
160
>>> exit()
[ladar@dark ~]$

Did the FBI Lean On Microsoft for Access to Its Encryption Software?



BY LORENZO FRANCESCHI-BICCHIERAI

SEP 11, 2013

"I realized that we were in this really interesting spot, sort of stuck in the middle between wanting to do a much better job at protecting our users' information, and at the same time realizing that this was starting to make government employees unhappy," Biddle said.

Despite Microsoft's refusals to backdoor its product, the engineers kept working with the FBI to teach them about BitLocker and how it was possible to retrieve data in case an agent needed to get into an encrypted hard drive.

At one point, the BitLocker team suggested the agency target the backup keys that the software creates. In some instances, BitLocker prompts users to print out a piece of paper with the key needed to unlock the hard drive, to prevent loss of data if a user forgets his or her key.

"As soon as we said that, the mood in the room changed dramatically," said the anonymous Microsoft engineer. "They got really excited."

In that instance, law enforcement agents wouldn't need a backdoor after all. As the engineer suggested, all they would need was a warrant to access a suspect's documents and retrieve the document that would unlock his or her hard drive.




Security For your life
1
2 ABC
3 DEF
ESC
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0/
M/OK



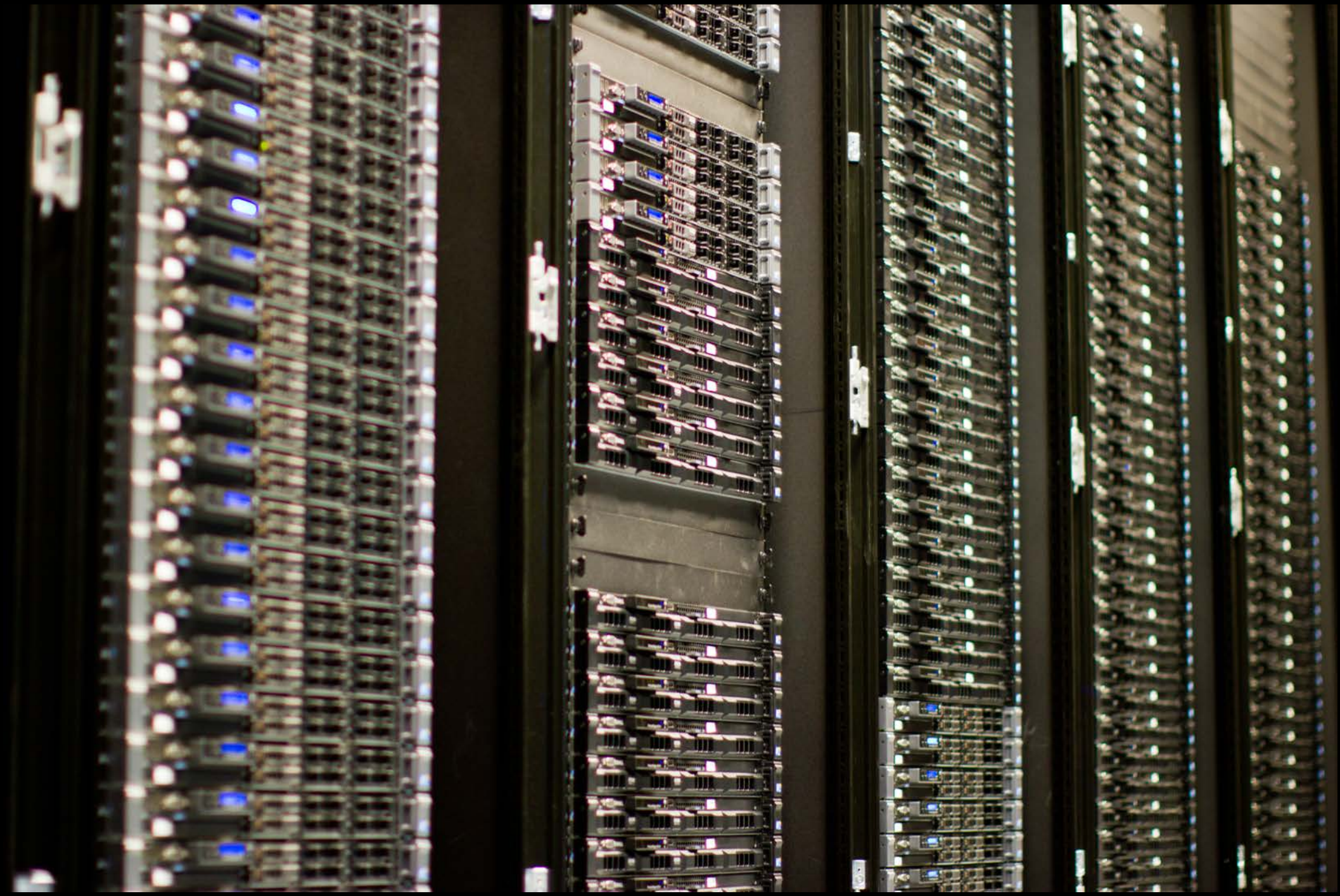
Third Parties

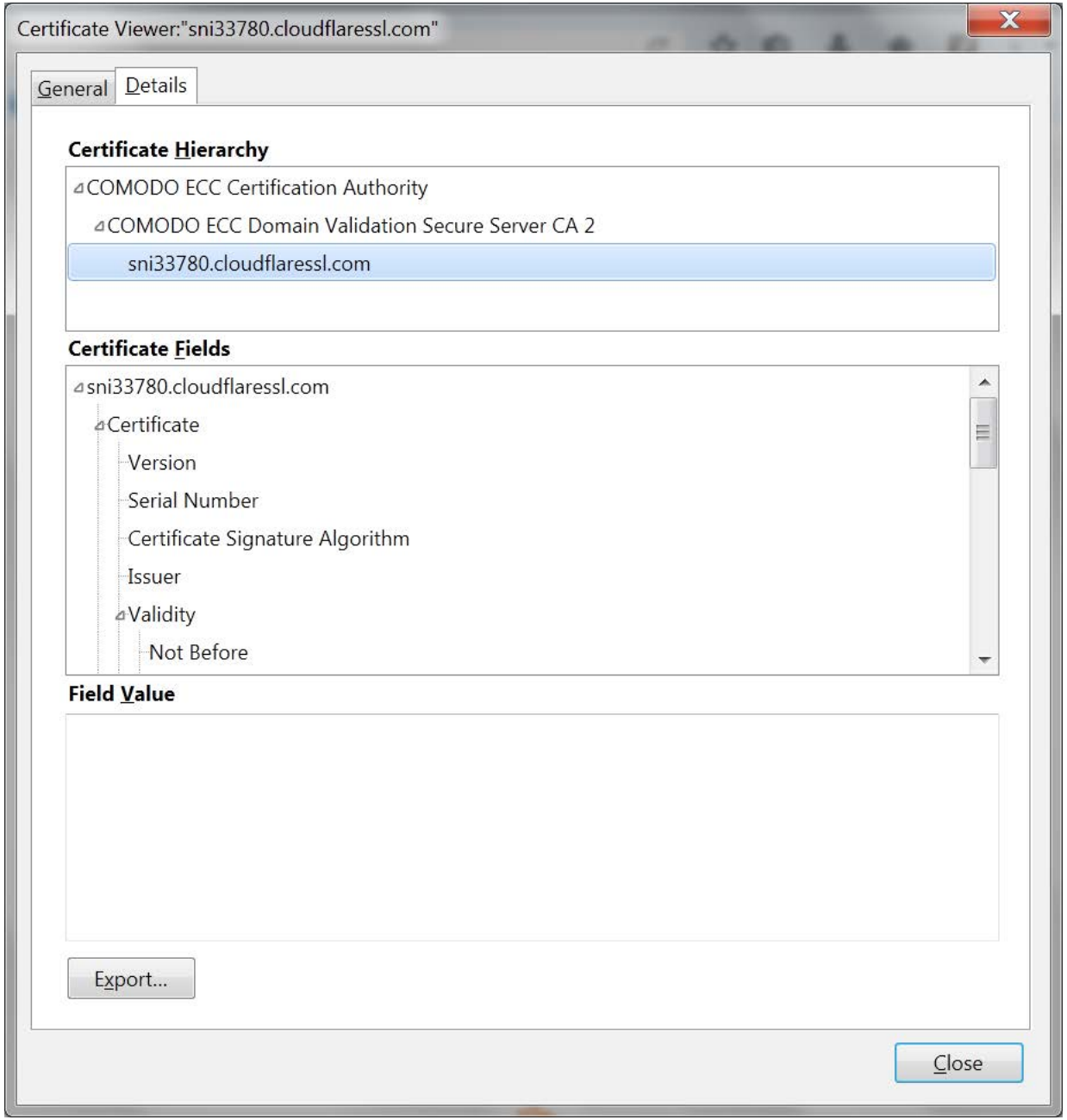
Like Lavabit, Apple, WhatsApp, Telegram, Dell, Cisco

or CentOS, OpenSSL CipherShed

or Linus Torvalds, Gavin Andresen, Werner Koch

or you




Certificate Viewer:"sni33780.cloudflaressl.com"
General
Details
Certificate Hierarchy
COMODO ECC Certification Authority
COMODO ECC Domain Validation Secure Server CA 2
sni33780.cloudflaressl.com
Certificate Fields
sni33780.cloudflaressl.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
Export...
Close


LINE 1
LINE 3
LINE 4
ON
OFF
FRONT
OF TAPE
REAR
OF TAPE

b. *Individuals Have a Diminished Expectation of Privacy in Email Communications with Non-U.S. Persons Outside the United States*

In evaluating the reasonableness of the incidental acquisition of non-targets' communications, I consider the degree to which U.S. citizens have a reasonable expectation of privacy in their email communications with non-U.S. persons abroad.

A person's expectation of privacy in email communications diminishes after sending the email because he or she assumes the risk that the recipient will share the communication with others. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("[An individual] may not . . . enjoy [] an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (email sender loses his or her legitimate expectation of privacy in an email that has already reached the recipient). Email communications are easily forwarded to or read by other parties. But this diminished expectation of privacy in email communications does not mean the government can search every email with impunity just because the email sender communicated with a foreign person abroad.[17]

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

As Apple Inc. concedes in its Opposition, it is fully capable of complying with the Court's Order. By Apple's own reckoning, the corporation—which grosses hundreds of billions of dollars a year—would need to set aside as few as six of its 100,000 employees for perhaps as little as two weeks. This burden, which is not unreasonable, is the direct result of Apple's deliberate marketing decision to engineer its products so that the government cannot search them, even with a warrant. Thus, the lawful warrant in this case—issued by a neutral magistrate upon a finding of probable cause, pursuant to the procedure blessed by the Supreme Court just two years ago in *Riley v. California*, 134 S. Ct. 2473 (2014)—will be frustrated unless Apple complies with the Order. In passing

3. Apple's Assistance Is Necessary

Without Apple's assistance, the government cannot carry out the search of Farook's iPhone authorized by the search warrant. Apple has ensured that its assistance is necessary by requiring its electronic signature to run any program on the iPhone. Even if the Court ordered Apple to provide the government with Apple's cryptographic keys and source code, Apple itself has implied that the government could not disable the requisite features because it "would have insufficient knowledge of Apple's software and design protocols to be effective." (Neuenschwander Decl. ¶ 23.)

MR. LEVISON: Before we do that, can I --

THE COURT: Well, what can I do about it if he doesn't, if he tells you he's not going to? You've got the right to go out and search and get it.

MR. TRUMP: Well, we can't get the information without his assistance. He's the only who knows and has possession of

it. We can't take it from him involuntarily.

also be added into the software.

In order to overcome these hurdles, the government seeks an order requiring Apple to assist in the execution of a search warrant using the capabilities that Apple has retained along within its encryption software, such that the government can attempt to determine the passcode without these additional, non-encryption features that Apple has coded into its operating system, for the SUBJECT DEVICE only. Apple's assistance would permit the government to electronically test passcodes without unnecessary delay or fear that the data subject to search under the warrant would be rendered permanently inaccessible. Given that these features were designed and implemented by Apple, that Apple writes and cryptographically signs the iOS, and that Apple routinely patches or updates its iOS to address security features or other functionality, modifying these features is well within its technical capabilities.

Specifically, in order to perform the search ordered in the warrant, the government requests that Apple be ordered to provide the FBI with a custom signed iPhone Software ("IPSW") file, recovery bundle, or other Software Image File ("SIF")[2] that can be loaded onto the SUBJECT DEVICE. The SIF would load and run from Random Access

is attempting to exercise in the case now before this court." The Supreme Court reversed, reaffirming two key principles: (1) congressional inaction, past or future, is uninstructive; and (2) because the AWA creates power *absent* congressional legislation, there is no need for Congress to specifically confer it. "Congress neither enacted nor rejected these proposals; it simply did not act on them. Even if it had, the legislation as proposed would have had no affect whatever on the power that Congress granted the courts by the All Writs Act. We cannot infer from the fact that Congress took no action at all . . . an intent to circumscribe traditional judicial remedies." *Id.* at 609. That holding was echoed in *New York Telephone*, which made clear that the AWA empowers a court to act "unless appropriately confined by Congress." 434 U.S. at 172-73.[2]

<page break removed>

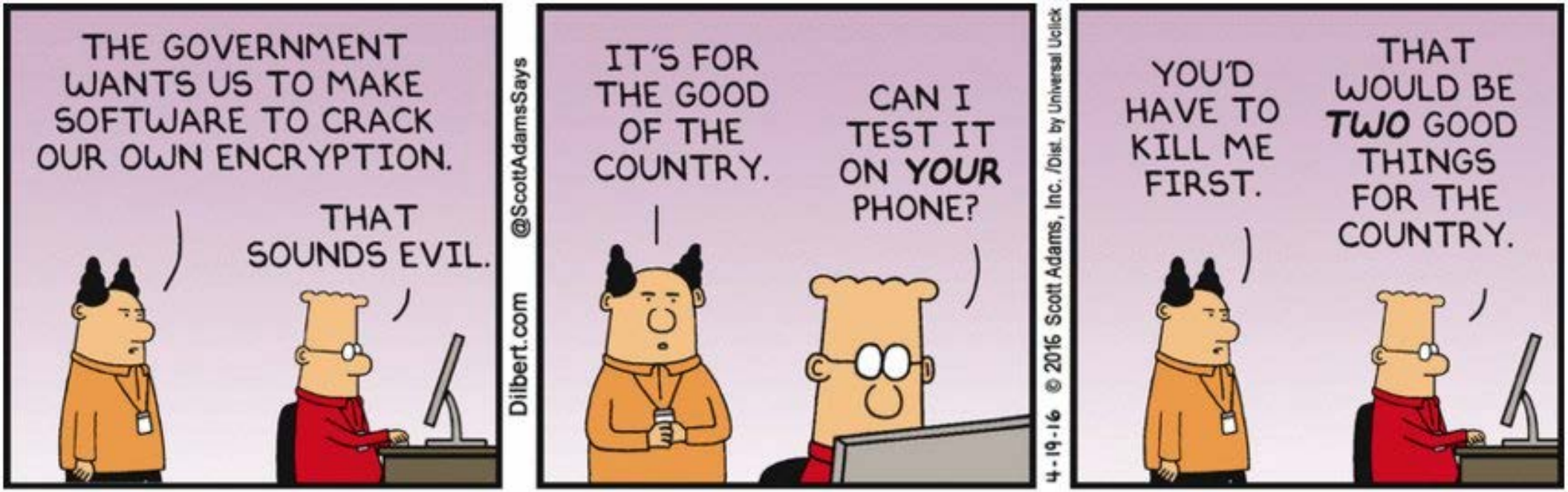
In short, the AWA does not require any *additional* legislation to empower the courts. Rather, as *Dean Foods* and *New York Telephone* held, the courts retain the flexible power bestowed by Congress through the AWA unless Congress expressly takes it away. As explained below, Congress has not enacted legislation that specifically confines the courts' power here. Its silence says nothing.


Medication Guide must be provided to
the patient upon dispensing.
NDC 59011-410-10
OxyContin®
(oxycodone hydrochloride
controlled-release) tablets
10 mg
Rx Only
100 Tablets
Purdue Pharma L.P.
WML81 EXP SEP14

is attempting to exercise in the case now before this court." The Supreme Court reversed, reaffirming two key principles: (1) congressional inaction, past or future, is uninstructive; and (2) because the AWA creates power *absent* congressional legislation, there is no need for Congress to specifically confer it. "Congress neither enacted nor rejected these proposals; it simply did not act on them. Even if it had, the legislation as proposed would have had no affect whatever on the power that Congress granted the courts by the All Writs Act. We cannot infer from the fact that Congress took no action at all . . . an intent to circumscribe traditional judicial remedies." *Id.* at 609. That holding was echoed in *New York Telephone*, which made clear that the AWA empowers a court to act "unless appropriately confined by Congress." 434 U.S. at 172-73.[2]

<page break removed>

In short, the AWA does not require any *additional* legislation to empower the courts. Rather, as *Dean Foods* and *New York Telephone* held, the courts retain the flexible power bestowed by Congress through the AWA unless Congress expressly takes it away. As explained below, Congress has not enacted legislation that specifically confines the courts' power here. Its silence says nothing.


THE GOVERNMENT WANTS US TO MAKE SOFTWARE TO CRACK OUR OWN ENCRYPTION.
THAT SOUNDS EVIL.
Dilbert.com
@ScottAdamsSays
IT'S FOR THE GOOD OF THE COUNTRY.
CAN I TEST IT ON YOUR PHONE?
4-19-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick
YOU'D HAVE TO KILL ME FIRST.
THAT WOULD BE TWO GOOD THINGS FOR THE COUNTRY.


And pay no attention to the little man behind the curtain...

ZDNet

US government pushed tech firms to hand over source code

Obtaining a company's source code makes it radically easier to find security flaws and vulnerabilities for surveillance and intelligence-gathering operations.



By Zack Whittaker for Zero Day | March 17, 2016 -- 16:30 GMT (09:30 PDT) | Topic: Security

NEW YORK -- The US government has made numerous attempts to obtain source code from tech companies in an effort to find security flaws that could be used for surveillance or investigations.

The government has demanded source code in civil cases filed under seal but also by seeking clandestine rulings authorized under the secretive Foreign Intelligence Surveillance Act (FISA), a person with direct knowledge of these demands told ZDNet. We're not naming the person as they relayed information that is likely classified.

With these hearings held in secret and away from the public gaze, the person said that the tech companies hit by these demands are losing "most of the time."

When asked, a spokesperson for the Justice Dept. acknowledged that the department has demanded source code and private encryption keys before. In a recent filing against Apple, the government cited a 2013 case where it won a court order demanding that Lavabit, an encrypted email provider said to have been used by whistleblower Edward Snowden, must turn over its source code and private keys. The Justice Dept. used that same filing to imply it would, in a similar effort, demand Apple's source code and private keys in its ongoing case in an effort to compel the company's help by unlocking an iPhone used by the San Bernardino shooter.



Why Apple went to war with the FBI

The Justice Dept. wanted to draw outrage, painting Apple as the criminal.

Asked whether the Justice Dept. would demand source code in the future, the spokesperson declined to comment.

IRATEMONK

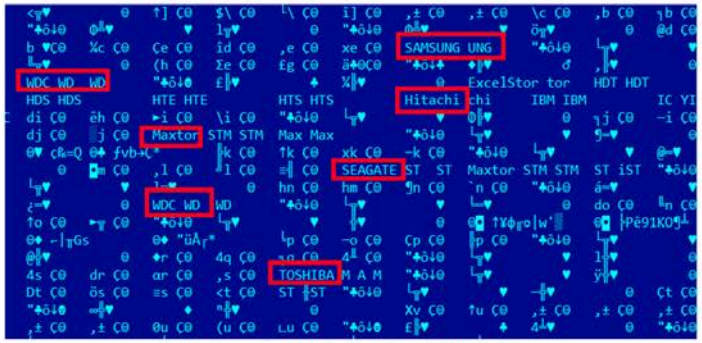
(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting in the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer).I Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

The plugin version 4 is more complex and can reprogram 12 drive “categories”.



Plugin version 4 infection “capabilities” table

The classes supported are:

- “WDC WD”, <Western Digital Technologies Inc> additional vendor specific checks used
- “ST”, “Maxtor STM”, “SEAGATE ST”, <Seagate Technology>
- “SAMSUNG”, <SAMSUNG ELECTRONICS CO., LTD.>
- “WDC WD”, <Western Digital Technologies, Inc.> additional vendor specific checks used
- <HGST a Western Digital Company>, “IC”, “IBM”, “Hitachi”, “HTS”, “HTE”, “HDS”, “HDT”, “ExcelStor”
- “Max”, “Maxtor STM”
- <MICRON TECHNOLOGY, INC.>, “C300”, “M4”
- <HGST a Western Digital Company>, <TOSHIBA CORPORATION>
- “OCZ”, “OWC”, “Corsair”, “Mushkin” additional vendor specific checks used
- <Samsung Electronics Co., Ltd., Storage System Division>, <Seagate Technology>, <SAMSUNG ELECTRONICS CO., LTD.> +additional checks
- <TOSHIBA CORPORATION COMPUTER DIVISION>, “TOSHIBA M” +checks
- <Seagate Technology>, “ST”

The main function to reflash the HDD firmware receives an external payload, which can be compressed by LZMA. The disk is targeted by a specific serial number and reprogrammed by a series of ATA commands. For example, in the case of Seagate drives, we see a chain of commands: “FLUSH CACHE” (E7) → “DOWNLOAD MICROCODE” (92) → “IDENTIFY DEVICE” (EC) → WRITE “LOG EXT” (3F). Depending on the reflashing request, there might be some unclear data manipulations written to the drive using “WRITE LOG EXT” (3F). For WD drives, there is a sub-routine searching for ARM NOP opcodes in read data, and then used further in following writes. Overall, the plugin uses a lot of undocumented, vendor-specific ATA commands, for the drives mentioned above as well as all the others.

The EQUATION group’s HDD firmware reprogramming module is extremely rare. During our research, we’ve only identified a few victims who were targeted by this module. This indicates that it is probably only kept for the most valuable victims or for some very unusual circumstances.

EQUATION GROUP: QUESTIONS AND ANSWERS

Version: 1.5
February 2015

#EquationAPT
#TheSAS2015



GREAT

KASPERSKY lab

ZDNet

US government pushed tech firms to hand over source code

Obtaining a company's source code makes it radically easier to find security flaws and vulnerabilities for surveillance and intelligence-gathering operations.



By Zack Whittaker for Zero Day | March 17, 2016 -- 16:30 GMT (09:30 PDT) | Topic: Security

NEW YORK -- The US government has made numerous attempts to obtain source code from tech companies in an effort to find security flaws that could be used for surveillance or investigations.

The government has demanded source code in civil cases filed under seal but also by seeking clandestine rulings authorized under the secretive Foreign Intelligence Surveillance Act (FISA), a person with direct knowledge of these demands told ZDNet. We're not naming the person as they relayed information that is likely classified.

With these hearings held in secret and away from the public gaze, the person said that the tech companies hit by these demands are losing "most of the time."

When asked, a spokesperson for the Justice Dept. acknowledged that the department has demanded source code and private encryption keys before. In a recent filing against Apple, the government cited a 2013 case where it won a court order demanding that Lavabit, an encrypted email provider said to have been used by whistleblower Edward Snowden, must turn over its source code and private keys. The Justice Dept. used that same filing to imply it would, in a similar effort, demand Apple's source code and private keys in its ongoing case in an effort to compel the company's help by unlocking an iPhone used by the San Bernardino shooter.



Why Apple went to war with the FBI

The Justice Dept. wanted to draw outrage, painting Apple as the criminal.

Asked whether the Justice Dept. would demand source code in the future, the spokesperson declined to comment.



Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens. All governments, democracies as well as autocracies, believe that those they seek to punish are guilty; the impediment of constitutional barriers are galling to all governments when they prevent the consummation of that just purpose. *But those barriers were devised and are precious because they prevent that purpose and its pursuit from passing unchallenged by the accused, and unpurged by the alembic of public scrutiny and public criticism. A society which has come to wince at such exposure of the methods by which it seeks to impose its will upon its members, has already lost the feel of freedom and is on the path towards absolutism.*

Judge Learned Hand

United States v. Coplon (1950)

REUTERS

Technology | Thu Mar 31, 2016 6:58pm EDT

Reddit deletes surveillance 'warrant canary' in transparency report

WASHINGTON | BY DUSTIN VOLZ



ars technica

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Reddit removes “warrant canary” from its latest transparency report

CEO is staying mum: "I've been advised not to say anything one way or the other."

by **Cyrus Farivar** - Mar 31, 2016 6:24pm CDT



Fin