The Digital Dark Arts

Mike Tigas, *ProPublica*
Nicole Hensley, *New York Daily News*
Defense Against the Dark Arts

Mike Tigas, ProPublica
What’s Really at Stake in the Apple Encryption Debate

The government has never been allowed to create a “backdoor” to encrypted devices. Now, it’s trying to force Apple to build one.

by Julia Angwin
ProPublica, Feb. 24, 2016, 3:29 p.m.

A protestor holds up an iPhone outside of the the Apple store on 5th Avenue on Feb. 23, 2016 in New York City. (Bryan Thomas/Getty Images)

The FBI’s much-discussed request to Apple can seem innocuous: Help us extract six
Court rules journalists can’t keep their sources secret

Published time: July 19, 2013 21:04
Edited time: July 20, 2013 16:41
Get short URL

Tags
CIA, Court, Crime, Iran, Nuclear, USA

A federal appeals court ruled Friday that New York Times journalist James Risen must testify in the trial of a former Central Intelligence Agency officer accused of leaking classified national defense information to the media.

A lower court ruled previously that Risen could protect the source responsible for sharing intelligence about a CIA operation discussed in his writing, but the US Court of Appeals from the Fourth Circuit reversed that decision Friday morning with a 2-1 vote.

“The reporter must appear and give testimony just as every other citizen must. We are not at liberty to conclude otherwise,” Chief Judge William Traxler Jr. wrote for the majority opinion.

The appeal panel’s decision came just days after United States Attorney General Eric Holder presented President Barack Obama with a proposal that would re-shape current law as it applies to journalists in order to more greatly ensure that reporters aren’t targeted during investigations unless other routes that exhausted first. That maneuver came on the heels of two highly public recent Justice Department scandals in which the White House was

1:07 PM - 16 Jan 2015

Pope: "World War III has begun"
NEVER CHAT

The Gawker-Hulk Hogan trial and the horror of work chats that stick around forever

by Ethan Chiel

March 9, 2016 12:03 p.m.

This week, Hulk Hogan's multi-million dollar lawsuit against Gawker for posting his sex tape finally went to trial. The Florida jury trial, with its testimony on penis size and extramarital sex, is almost as NSFW as the video itself, an excerpt of which Gawker posted in 2012—and then took down after being sued. But what was really on our minds watching the proceedings via livestream is the reminder that every time you send an email to a coworker or type a message in an intra-office chat room you should imagine that someday your words will be read out loud in open court.

Threat Modeling

• Basically the who/what/where/when/why/how of thinking about security & risk. Some examples of Qs you might ask:

  • Why might you be targeted?
  • Who are your enemies?
  • What might be used against you?
  • What could go wrong in your day-to-day?
  • How secure do you need it?
Technical
• crypto
• hacking, intercepted communications, code-breaking

Legal
• legal protections
• lawsuits, subpoenas, detention

Social
• phishing, "social engineering," exploiting trust

Physical
• locks, security guards
• theft, network taps, torture

Operational
• how do you put the above into action?
• how do you go about your business?
• shit happens, do you have a backup plan?
Computers: How do they work?
Data at rest. What's on your computer? What's sitting in your e-mail archive?
Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Communication! Calls, messages, files sent; anything out of your hands.
Plain Old Telephone Service (POTS) Networking

1. Calls sent
2. Calls received
3. Switch
4. Central Office Phone Co.
5. Transport
6. Terminal

https://www.mackinac.org/6765
https://en.wikipedia.org/wiki/Grumman(LLV)
John H. Atherton  
Dept. of Anth.  
Portland State U.  
P.O.Box 751  
Portland, Oregon, 97207  
U.S.A.
Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Communication! Calls, messages, files sent; anything out of your hands.

Metadata. Who are you talking to & when. How big are those files/msgs?

http://www.salon.com/2013/04/24/how_a_twitter_hack_sent_the_market_plummeting_ap/
**Data at rest.** What's on your computer? What's sitting in your e-mail archive?

**Data in motion.** Calls, messages, files sent; anything out of your hands.

**Metadata.** Who are you talking to & when. How big are those files/msgs?

**Identities & logins.**
WASHINGTON (AP) — The Justice Department secretly obtained two months of telephone records of reporters and editors for The Associated Press in what the news cooperative's top executive called a "massive and unprecedented intrusion" into how news organizations gather the news.

The records obtained by the Justice Department listed outgoing calls for the work and personal phone numbers of individual reporters, for general AP office numbers in New York, Washington and Hartford, Conn., and for the main number for the AP in the House of Representatives press gallery, according to attorneys for the AP. It was not clear if the records also included incoming calls or the duration of the calls.

In all, the government seized the records for more than 20 separate telephone lines assigned to AP and its journalists in April and May of 2012. The exact number of journalists who used the phone lines during that period is unknown, but prosecutors clearly had an interest in the reporters who used them.
Police subpoena KMSP Minneapolis reporter's cell records

Associated Press, December 13, 2007 7:56 AM EST

ST. PAUL, MINN. (AP) — St. Paul police subpoenaed the cell phone records of a KMSP-TV reporter and the phone records of a Ramsey County sheriff's department employee after the reporter obtained an arrest report that should have been public data, the station reported Tuesday night.

Veteran police reporter Tom Lyden had gone to the police department to check on the criminal history of a woman who was sitting in a car with a man who allegedly shot an undercover police officer in a roadside incident in Coon Rapids last June, the station reported.
Never Chat

The Gawker-Hulk Hogan trial and the horror of work chats that stick around forever

by Ethan Chiel

March 9, 2016 12:03 p.m.

This week, Hulk Hogan’s multi-million dollar lawsuit against Gawker for posting his sex tape finally went to trial. The Florida jury trial, with its testimony on penis size and extramarital sex, is almost as NSFW as the video itself, an excerpt of which Gawker posted in 2012—and then took down after being sued. But what was really on our minds watching the proceedings via livestream is the reminder that every time you send an email to a coworker or type a message in an intra-office chat room you should imagine that someday your words will be read out loud in open court.

Technical
• crypto
• hacking, intercepted communications, code-breaking

Legal
• legal protections
• lawsuits, subpoenas, detention

Social
• phishing, "social engineering," exploiting trust

Physical
• locks, security guards
• theft, network taps, torture

Operational
• how do you put the above into action?
• how do you go about your business?
• shit happens, do you have a backup plan?
People are insecure.
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.

http://xkcd.com/538/
Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hello,

Please read the following article, it's very important:


[A different AP staffer]
Associated Press
San Diego
mobile [removed]
Microsoft®
Outlook Web App

Your session has timed out. To protect your account from unauthorized access, the connection to your mailbox is closed after a period of inactivity. Please re-enter your user name and password.

Security (show explanation)
- This is a public or shared computer
- This is a private computer
- Use the light version of Outlook Web App

Domain/user name: [input field]
Password: [input field]

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.
HACKED BY SEA

- Dracula’s Missile Defense
- Star Wars: Images of the Perseid Meteor Shower
- Brooklyn Man Electrocuted After Urinating on Subway’s ‘Third Rail’
- How a Beige Book Could Shed Light on China’s Shadow Economy
- Japan Unveils the Izumo, Its Largest Warship Since WWII, Amid Tensions With China
- 6 Things Not Worth the Money (Reader’s Digest)
- Why China’s Renewable Energy is in the World’s Best Interest (DwFaq)
- RA and Sex: Relationships Matter (Health Central)
- 10 Cheapest Places to Take a Vacation (TripGens)
- Cancer Hates Oxygen — Here’s Why (Revolar)

2 Comments
Technical
• crypto
• hacking, intercepted communications, code-breaking

Legal
• legal protections
• lawsuits, subpoenas, detention

Social
• phishing, "social engineering," exploiting trust

Physical
• locks, security guards
• theft, network taps, torture

Operational
• how do you put the above into action?
• how do you go about your business?
• shit happens, do you have a backup plan?
$ whois miketigas.com

Domain Name: MIKETIGAS.COM
Registry Domain ID: 554945391_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2015-07-16T10:19:23.0Z
Creation Date: 2006-08-15T05:48:36.0Z
Registrar Registration Expiration Date: 2016-08-15T05:48:36.0Z
Registrar: DYNADOT LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: M. Tigas
Registrant Street: PO BOX 426
Registrant City: NEW YORK
Registrant State/Province: NY
Registrant Postal Code: 10014-0426
Registrant Country: US
Registrant Phone: +1.3476884427
Registrant Email: mike.tigas@propublica.org
Vehicle Purchase Records Data Search

FIRST NAME: JOHN
LAST NAME: DOE

SEARCH NOW

http://vin.place/
1 results found for Michael Tigas

MICHAEL TIGAS
Purchase of a 2012 TOYOTA PRIUS C

VIN: JTDKDB3XC101XXXX

http://vin.place/
Customer Name: MICHAEL TIGAS

- Address: 11 Dogwood Ter
- City: Livingston
- State: NJ
- Zip: 07039-3601
- Phone: 573864XXXX
- Year: 2012
- Make: TOYOTA
- Model: PRIUS C
Tools and concepts that can help
Look for your own metadata footprint

- Search yourself in “people finder” sites & opt-out of your data showing up:
  - https://crashoverridenetwork.tumblr.com/post/108387569412/preventing-doxing
Software updates, Antivirus/antispyware

Security holes in Windows, Mac, and Linux, are discovered on a near-daily basis. Same with browsers and most other software. (When it annoys you to restart & update, just do it!)
Passwords

Don't use the same couple of passwords everywhere.

Your e-mail password needs to be stronger than your bank's. (At least you can call up your bank for help if there's fraud. Not so much w/e-mail.)

E-mail owns your other accounts — nearly every website has an “I forgot my password” feature that e-mails you.
Passwords

An 8 letter password with numbers and symbols can be cracked in a few days, but an 8 word phrase could take centuries.

“Pass phrases” – use a real sentence instead of just one word. Google and Twitter (& many others) let you use a password as long as you want!

Unfortunately, websites don't always let you do this.
Tr0ub4dor & 3

~28 bits of entropy

2^28 = 3 days at 1000 guesses/sec

Difficulty to guess: EASY

Was it trombone? No, troubador. And one of the Os was a zero?

And there was some symbol...

Difficulty to remember: HARD

Correct horse battery staple

~44 bits of entropy

2^44 = 550 years at 1000 guesses/sec

Difficulty to guess: HARD

That's a battery staple. Correct!

Difficulty to remember: You've already memorized it

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Password Managers

Helps you use a different password everywhere. Can generate totally random passwords for every website.

**1Password** (Mac/iOS/Windows)

**LastPass** (multiplatform, website)

**KeePassX** (multiplatform app)
Two Factor Login

• Helps keep an account secure, even if your password is stolen.

• First factor: “something you know” (your password)

• Second factor: “something you have” (your phone)

• You (or an evildoer) need both to get into your accounts.

• Google has it, Yahoo has it, Twitter, Facebook, Dropbox, lots of banks.
Two Factor Login

Google 2-Step Verification

Enter the verification code generated by your mobile application.

Enter code

Verify

- Remember this computer for 30 days.

Problems with your code?
Secure deletion

• When you delete a file from your computer, you’re only deleting it from the “table of contents” of your drive.

• Data still there until something else needs to use those unused “pages.”

• A “secure” delete writes random data into the place where the file was.
Secure deletion

• Erasing files:
  • “Secure Empty Trash” on Mac: hold ⌘ key when right-clicking Trash.
  • CCleaner (Windows)

• Erasing free space (to wipe files that you didn’t erase securely):
  • Disk Utility (Mac)
  • CCleaner (Windows)
File encryption

• Protects files

• Use case: sending sensitive files or putting files on USB sticks to share.

• TrueCrypt (multiplatform)

• MiniLock (multiplatform)
Full disk encryption

• Protects all data on your computer, when computer is turned off.

• Use case: Protects if computer is stolen

• Apple FileVault (Mac)

• BitLocker (Windows “Pro” or “Enterprise” versions)
FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".
BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

TPM Administration
Disk Management
Privacy statement
But what about other tools?

- New tools come out all the time.
- We don’t necessarily know what’s secure. Follow a lot of security experts to see what their consensus is.
- Consider the encryption, metadata-masking capabilities, and transparency of how tools work:
  - https://projects.propublica.org/graphics/privacy-tools
Further reading

Freedom of the Press Fdn. encryption guide

Threat Modeling guide on OpenNews Source
Continued…

- The Digital Dark Arts (Part 2):

- CryptoParty slides about tools:
Other relevant sessions

• CryptoParty
  • Saturday, 2:15PM, Colorado B-D (near exhibitors)
    • http://www.ire.org/events-and-training/event/2198/2459/

• Seeing like a network: Learning how to think about digital security
  • Sunday, 9:00, Penrose room
    • http://www.ire.org/events-and-training/event/2198/2399/