When the Cops Come A-Knocking: Handling Technical Assistance Demands from Law Enforcement

Jennifer Granick & Riana Pfefferkorn
@granick & @riana_crypto
Stanford Center for Internet and Society

This Talk

- ✓ Identifying legal and business issues when police ask for technical assistance in lawfully collecting information about your users

- X NOT when you're obligated to turn over user information you have
- X NOT about foreign governments or intelligence agencies
- X NOT legal advice

Traditional Technical Assistance

Law enforcement:

- Obtains a court order *ex parte* (only the government appears in court)
- Order is signed by judge or magistrate
- Order requires technical assistance under Pen Register Statute or Wiretap Act (Title III)
- Delivers order to communications provider (local phone company)

Traditional Technical Assistance

Provider:

- Is served with and reviews the order
- Controls computer interface capable of electronically delivering call info (numbers dialed + audio of call) over leased line to LE monitoring facility
- “Flips the switch” to send data over LE line to LE facility

Novel Technical Assistance?

- Decrypt data
- Write new software to circumvent security
- Turn on microphones or video cameras
- Disclose private encryption keys
- Build in backdoors

Technical Assistance Demands

- Not new
- LE is more aggressive because of encryption and “Going Dark”
- Lack of clear rules for Internet companies on when technical assistance is required
- LE takes advantage of uncertainty
- Companies can (and should) push back

Special Case: CALEA

- Statute mandates wiretappability
- Applies to telephone companies, interconnected VoIP, broadband Internet, and replacements for phone per FCC
- Does not apply to “information services”
- Must follow technical standard

CALEA & Encryption

Even regulated entities do not have to be able to decrypt unless they *both*

- provide encryption **and**
- possess the information necessary to decrypt

Does Anyone Else Have To Decrypt?

Do NOT have to build in decryption capabilities

If you *could* decrypt, then ask:

Relevant Statutes

- Pen Register Statute: 18 USC 3121 *et seq.*
- Wiretap Act: 18 USC 2511 *et seq.*
- All Writs Act (AWA): 28 USC 1651

If there's no statutory authority to compel assistance, then you don't have to assist

Pen Register/Wiretap Act

- a provider or other person
- shall furnish technical assistance
- necessary
- unobtrusively
- and with a minimum of interference

All Writs Act (1789) (AWA)

"The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

Be Prepared

- Familiarize yourself with the history and the law
- Know your product/service
- Have a plan

Know Your User Data Practices

- What do you collect?
- What do you store?
- For how long?
- Why?
- What can your company access?
- What do you encrypt?
- Where are the keys?

Have good reasons for privacy/security designs

Who You Gonna Call?

- Have a game plan in place beforehand
- Identify knowledgeable in-house & outside counsel
- Ensure that CSO/CISO will be involved in the decision

Technical Assistance Orders

- Provide cleartext you already have – YES
- Decrypt – Unknown (caveat: CALEA)
- Write new software – Unknown
- Turn on microphone or camera – Unknown
- Hand over your encryption keys – Unknown
- Create “backdoors”/design for wiretappability – NO (caveat CALEA)
- Allow the government to install its equipment or software on your premises or systems – NO

Decryption?: Data with Providers

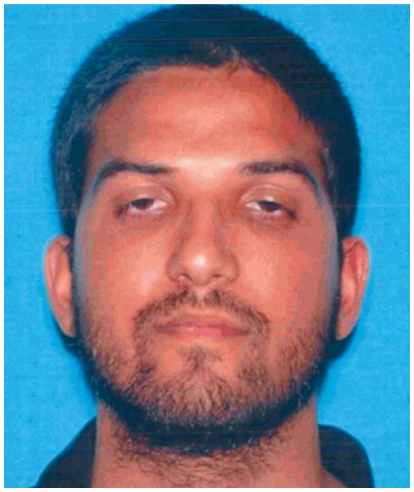
- General practice:
  - If provider has the data and can decrypt it, generally they do so
- Authority:
  - Pen Register/Wiretap Act OR
  - Stored Communications Act + AWA (express/ implied)
- Is this correct under the law? *Unknown*

Decryption?: Data on Devices

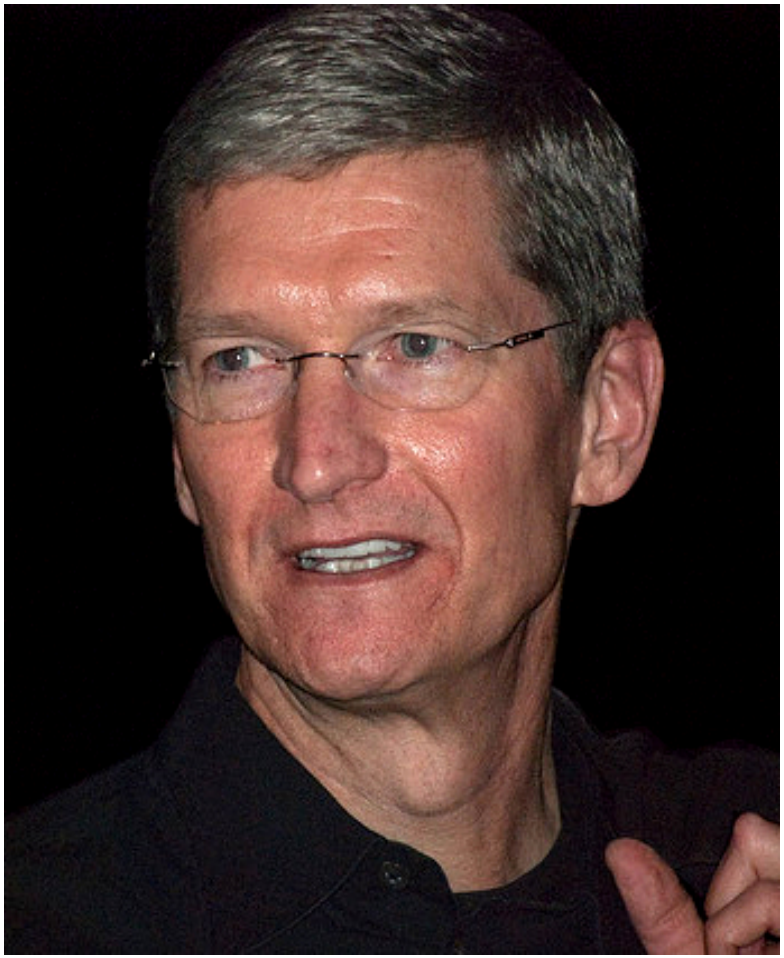
- No direct statutory authority
- DOJ: search warrant **plus** AWA
- Brooklyn Apple v. FBI case: Can AWA compel decryption? *Unknown*

Create New Software?

- San Bernardino Apple v. FBI case: Can AWA compel creation of new software? *Unknown*



Apple v. FBI



New York Telephone (1977)

- Installing pen registers at phone company
- Gov won: phone company forced to install
- Basis for law enforcement's present-day All Writs Act theory

Turn on Audio or Video?

- *The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003)
- Pen Register statute, Wiretap Act
  - Similar technical assistance language
- Three issues:
  - "other person"
  - Necessary?
  - Unobtrusive + minimum of interference?
- *Unknown*

Smart TVs

Voice Recognition

You can control your SmartTV, and use many of its features, with voice commands.

If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

Disclose Encryption Keys?

- AWA/Pen Register/Wiretap Act
  - Necessity?
  - Burden?
- Do courts consider privacy and security dangers?
- Seizure Warrant
  - Keys are not evidence of a crime/contraband

Unknown

Lavabit

Pen Register/Trap & Trace

"a provider … shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services"

SCA Seizure Warrant

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Lavabit, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All information necessary to decrypt communications sent to or from the Lavabit e-mail account [redacted] including encryption keys and SSL keys;

b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]

Malicious Software Update?

- Compel code signing key?
- In addition to the lack of statutory authority, First Amendment issues

Backdoors?

- *NO.* No obligation for non-CALEA entities to design to be surveillance-friendly.
- [No obligation for CALEA entities to ensure decryptability if they do not both provide the means and have the keys.]

End-to-end encryption is legal.

Period.

Backdoors

If you build it, they will come

Gov't Software/Direct Access

- No statutory authority
- The point of CALEA was to avoid this outcome
- Very dangerous
- At minimum CSO/CISO, General counsel approval, code review, etc.
- So, No.

Legal Summary

- Historically very little companies are obligated to do
- Requests are not orders
- Orders are not the law
- Unsettled authority — exercise independent judgment
- Embrace encryption
- Some legal issues are appropriateness, necessity, burden, security

So You've Received a Technical Assistance Order.

Now What?

Checklist

- Read the Order
- Is it signed by a judge?
- Are the police asking for only what the order says?
- If AWA is there also a surveillance order?
- Ask them to go back to court for more explicit authority?
- Ask for notice and an opportunity to be heard?

Checklist pt. 2

- What does the order require?
- Hand over cleartext – see ECPA etc. No novel technical assistance issue
- Decrypt & disclose, you are the provider, and you have the key – Likely the same, see ECPA
- Gag order?
- Novel technical assistance: Call the lawyers

Checklist pt. 3
Novel Tech Assistance Orders

Law almost certainly does not require compliance. So:

- Involve legal and security experts
- Would compliance be burdensome?
- Would compliance interfere with the product/ service?
- Would compliance be bad for business/security?
- Are there other feasible alternatives?
- How strong are legal arguments on each side?

Should You Push Back?

Your Mileage May Vary

- Strength of legal arguments
- Company's resource levels
- Relationships with law enforcement
- Future demands from US and other governments
- Public relations

Costs of Compliance

- Government compensates for “reasonable expenses incurred” in providing technical assistance.

Conclusion

- If you get an overreaching demand:
  - Push back intelligently where possible
  - Talk about the demands you get, if you can

Questions?