
# White Hat Privilege

## The Legal Landscape for a Cybersecurity Professional Seeking to Safeguard Sensitive Client Data

GOODWIN

Karen L. Neuman
Jacob R. Osborn

7/27/2017

# White Hat Privilege

## What legal or technical tools can security experts use to protect customer data?

# Protect Sensitive Customer Data from Whom?

- The public
  - Third parties (e.g., competitors)
- Bad actors
  - Hackers, enemies, opportunists
- The government
  - Courts, law enforcement

# Tool #1: Privilege

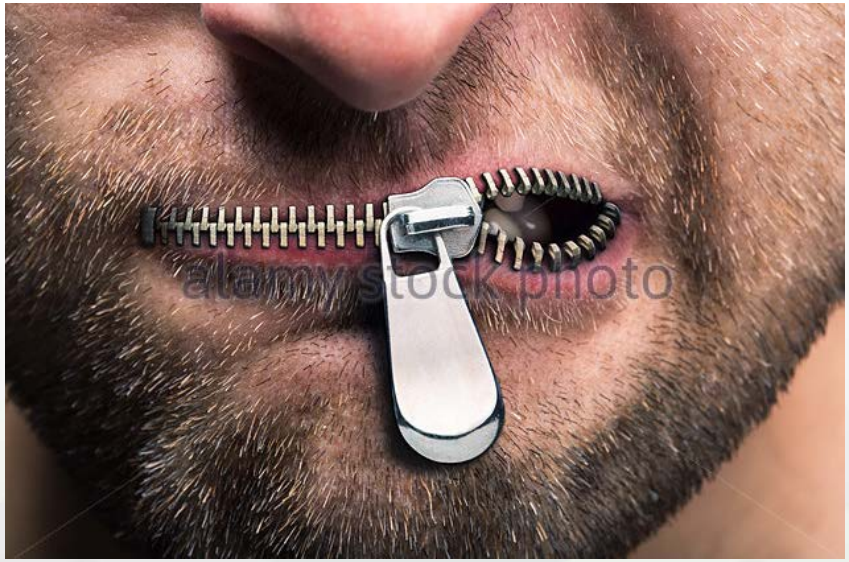
- Limited evidentiary protections
- Protects against disclosure to the government or to third parties in an adversarial context
  - Criminal cases
  - Civil cases
  - Subpoena demands

# Attorney-Client Privilege

- "A gentleman does not give away matters confided to him."
  - Hazard, Geoffrey C. Jr., "An Historical Perspective on the Lawyer-Client Privilege" (1978), *Yale Law School Faculty Scholarship Series*, Paper 2406.

# Lawyer's Duty of Confidentiality

- "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . ."
  - American Bar Association Model Rules of Professional Conduct, Rule 1.6.



## Security Consultant - Client Privilege???

- Nope

## *In re Experian Data Breach Litigation* (C.D. Cal., May 18, 2017)

- Experian suffered data breach
- Experian immediately hired outside legal counsel, who retained Mandiant to investigate
- Class action lawsuit against Experian
- Experian's lawyers refused to provide the Mandiant report and documents to plaintiffs
- Mandiant report and documents protected under work product performed in "anticipation of litigation"

# Takeaway

- Consider when a situation might benefit from attorney-client privilege or work-product privilege.
- Get outside lawyers involved early to help navigate how to protect information from legal demands.

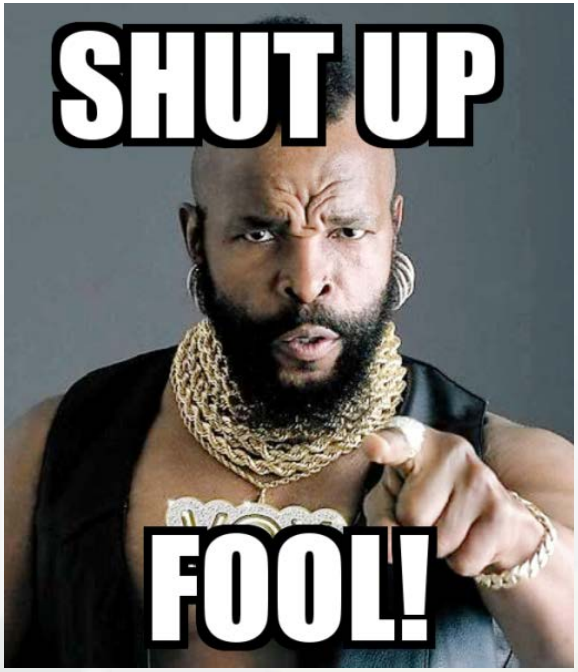
# Tool #2:  Contractual Protections

# It’s all about the contract, dummy.

- DTR talk
  - Who will be performing the services?
  - What will they be doing?
  - What tools will they use?
  - Where will they be doing it?
  - When is it to be done?
  - What is the end product?

# It’s all about the contract, dummy.

- Keep yo’ trap shut.
  - Confidentiality clauses
  - NDAs



# It’s all about the contract, dummy.

- Oops, did I do that?
  - Allocate risk and limit liability
  - Insurance coverage?

# It’s all about the contract, dummy.

- That’s mine!
  - Intellectual property ownership and use

# It’s all about the contract, dummy.

- Termination clause
  - When you discover you are married to a Scientologist

# It’s all about the contract, dummy.

## BAD CONTRACT

USE SMALLER FONT

## GOOD CONTRACT

USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT
USE SMALLER FONT

# But not ALL about the contract, dummy.

- Data privacy laws and regulations
- Export control regulations
- Financial regulations
- Healthcare data regulations
- Public company regulations
- Subpoenas; technical assistance demands
- Etc.

# But not ALL about the contract, dummy.

- Data privacy laws and regulations
  - Interests are mostly aligned – security for individuals' personally identifiable information
  - What about data breach notification laws?
    - State law

# But not ALL about the contract, dummy.

- Export control laws
  - ITAR-controlled data or technology?
  - EAR controlled technology?


# But not ALL about the contract, dummy.

- Pay attention to Wassenaar
  - “Intrusion software” controls?
  - 0-day exploits and related technology

## Tool #3: Technical Mechanisms

- Can protect against:
  - Public
  - Bad actors
  - The government

## Tool #3: Technical Mechanisms

- Identify where information is stored
  - Internal corporate network
  - Private servers
  - Public/private cloud
  - Email
  - Chat (slack, basecamp, hipchat)
  - Laptops
  - Other mobile devices (text?)

## Tool #3: Technical Mechanisms

- Identify where information is stored
  - Internal corporate network
  - Private servers
  - ~~Public~~/private cloud
  - Email
  - ~~Chat (slack, basecamp, hipchat)~~
  - Laptops
  - Other mobile devices (~~text?~~)

# Physical movement of electronic devices

- What are your rights if government agents want to search your electronic devices?

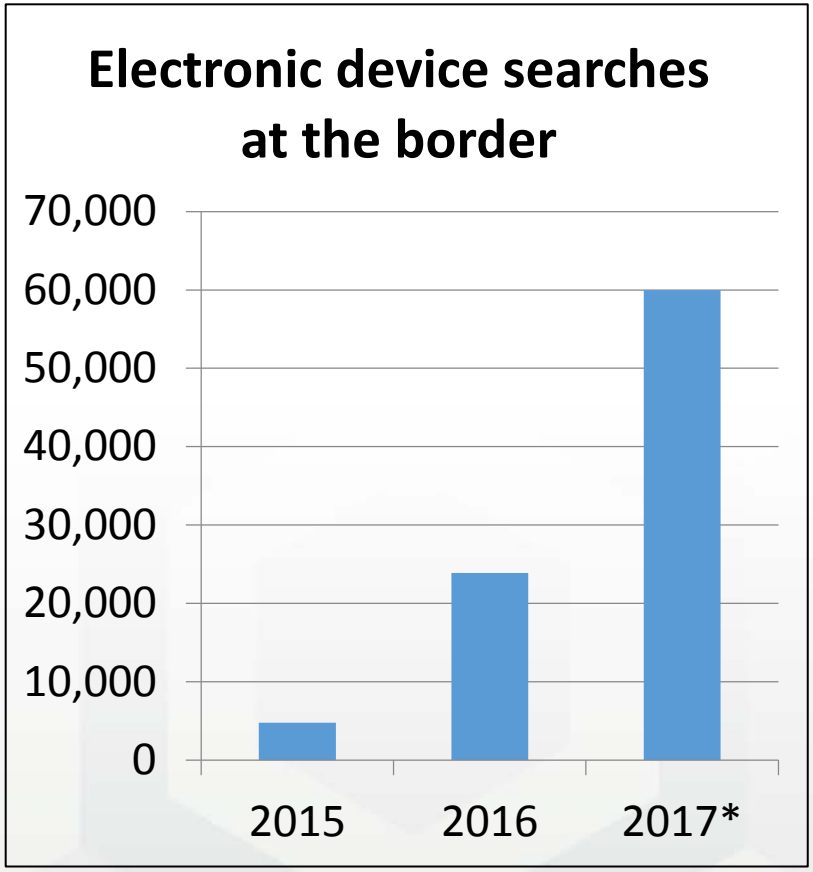
# Domestic travel

- Department of Homeland Security (DHS)
  - Transportation Security Administration (TSA)
    - Charged with “screening” for safety at the airport
    - No right to conduct a comprehensive “search” of data on your electronic devices
    - Constitutional protections apply to domestic travel

# Entry into the United States

- Department of Homeland Security (DHS)
  - Customs and Border Protection (CBP)
    - Limited Legal Protections
    - DHS Privacy Impact Assessment for the Border Searches of Electronic Devices and CBP fact sheet

# Hand over your device; give me your data




*2017 data projection

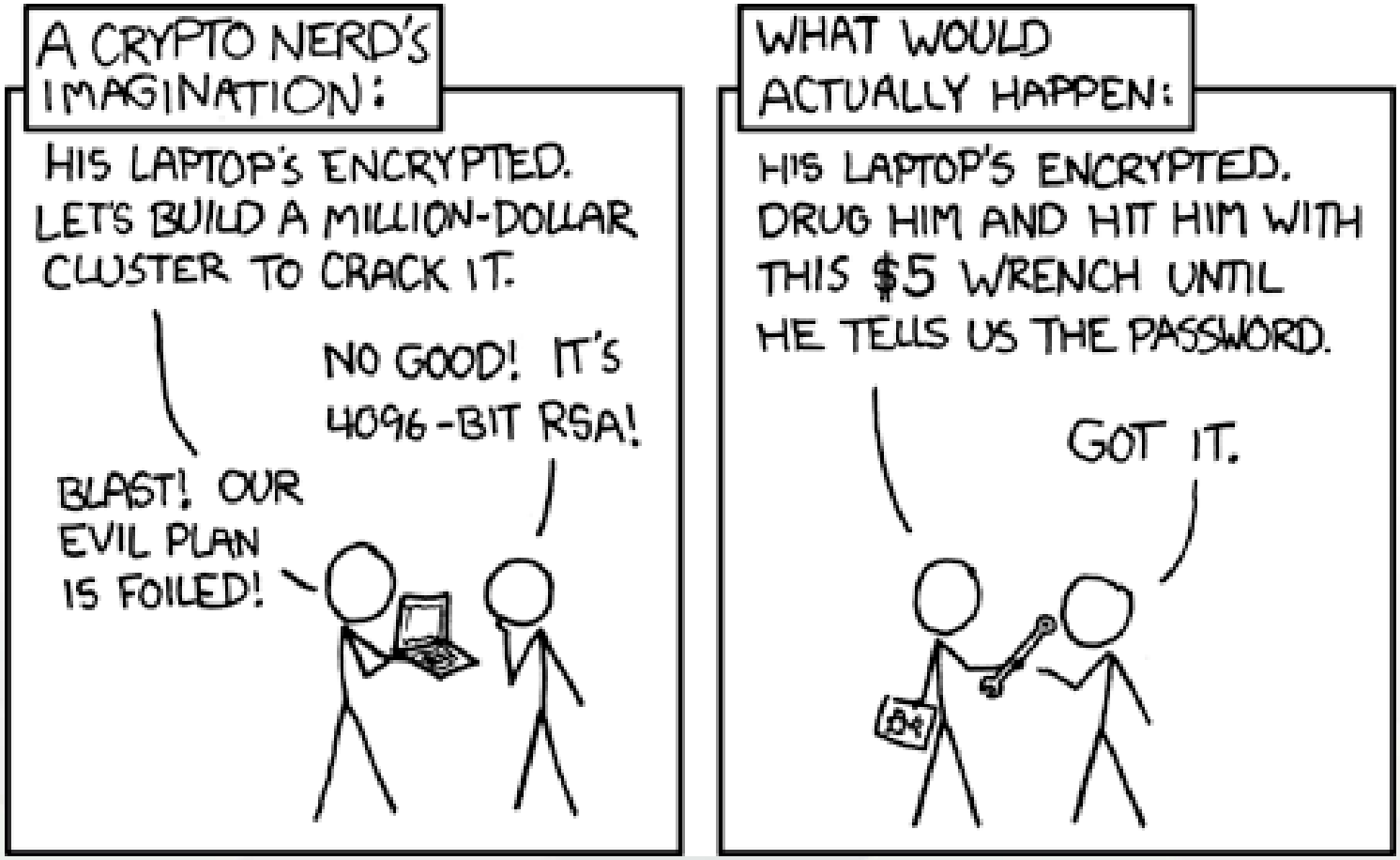
# Hand over your device; give me your data

- Think you can say no?
  - CBP has broad authority at the border
  - Limited 4th amendment protection
  - Broad authority to conduct cursory searches
  - Forensic searches more limited in *some states*

# Hand over your device; give me your data

- Hold up a minute . . .
  - Destroying evidence: CRIME
  - Making a false statement: CRIME
  - Taking the device?
    Get a receipt.
  - Withholding your password
- Don’t count on legal protections

# Hand over your device; give me your data



# Hand over your device; give me your data

- Takeaway
  - Don’t count on legal protections
  - Don’t make false statements
  - Don’t destroy evidence

# Hand over your device; protect your data

- Limit data stored and downloaded on the device
- All device data should be encrypted
- Disable automatic logins to email, cloud storage and social media
- Don’t give your password
- Assert privilege?
- Contact employer or lawyer
- Make them work for it
- Be creative . . .

# Technical tools

- Encrypt data and separately send key?
- Other technical tools to encrypt data for device transport
  - 1password Travel Mode tool
  - Kali Linux Full Disk Encryption with LVM / LUKS NUKE feature


# The End

GOODWIN

Karen L. Neuman
kneuman@goodwinlaw.com

Jacob R. Osborn
josborn@goodwinlaw.com
@jacobrosborn