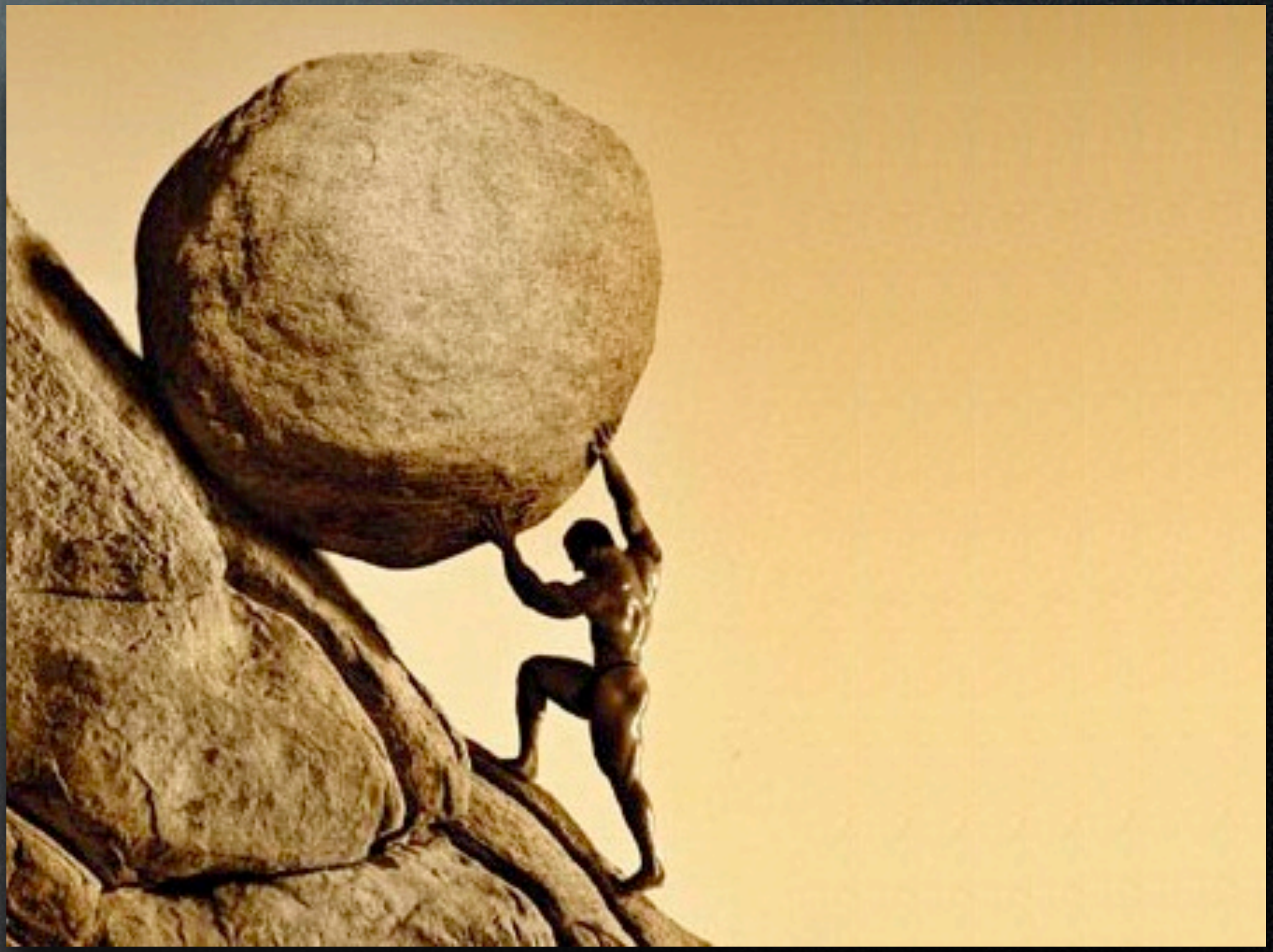
# The Cybersecurity Landscape

Ronald L. Chichester, JD, CFE, CISA
Ronald Chichester, P.C.

Advanced Business Law Seminar
Houston, Texas
November 19, 2015

# Overview

- The Current Situation
- The Breach
- The Discovery
- The Confession
- The Consequences
- The Aftermath



# Cast of Characters

- The Miscreant(s)
- The IT Person(s)
- Law Enforcement
- The Management
- The Lawyer(s)
- Agency Lawyer(s)
- Investors

# The Current Situation

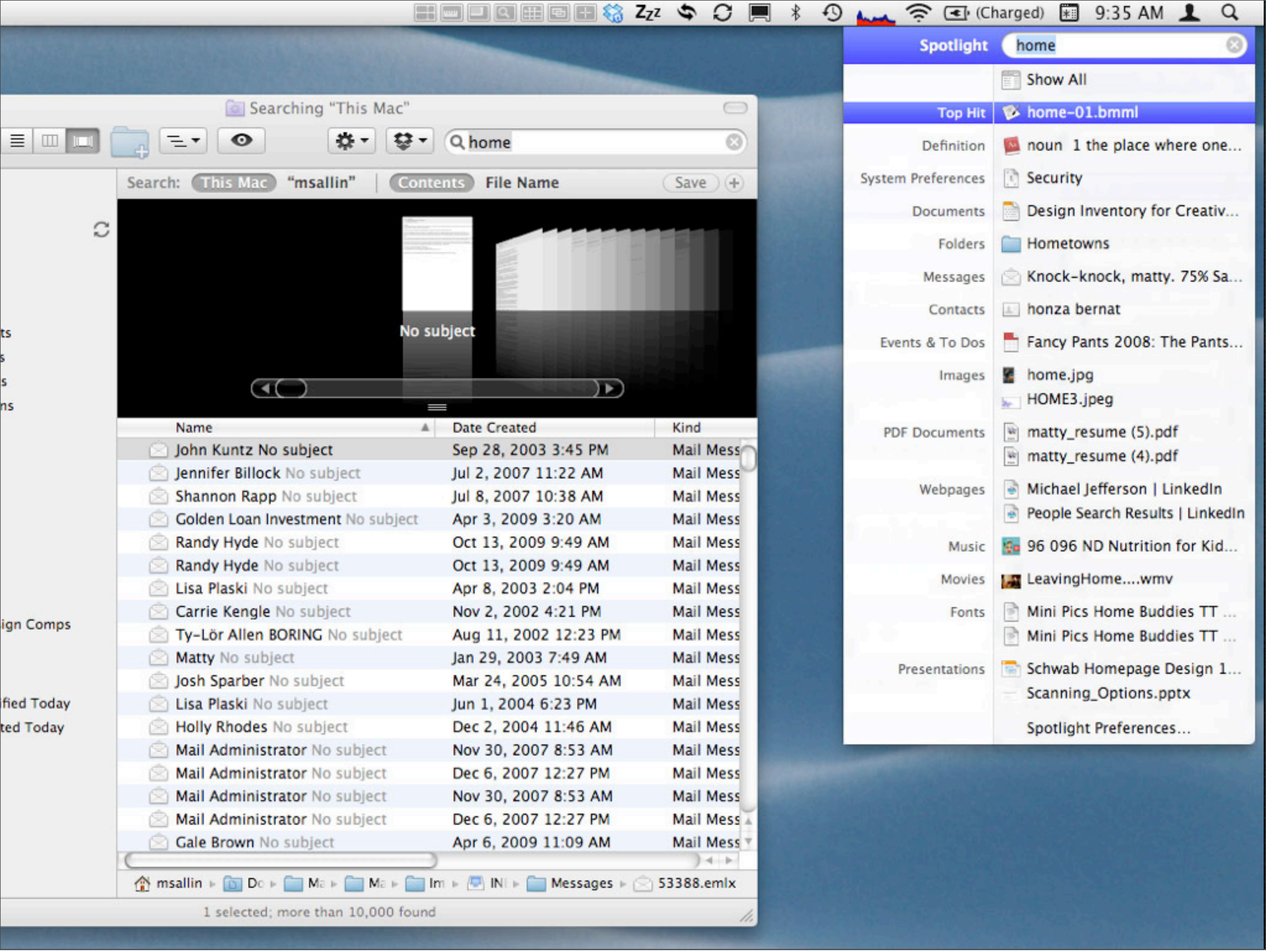
- It’s bad
- … and it will get MUCH worse
- The DR’s are not the only concern

# The Current Situation

- NSA broke into 50,000 networks (worldwide) and planted malware
- Other State Threat Actors
- Low cost of entry
- Far more sophisticated malware

# Points of Vulnerability

- Windows & OS X
- Unencrypted files
- Unencrypted databases
- Unencrypted backups
- System Indexes



Searching "This Mac"

home

Search: This Mac "msallin" | Contents File Name Save

No subject

| Name | Date Created | Kind |
|---|---|---|
| John Kuntz No subject | Sep 28, 2003 3:45 PM | Mail Mess |
| Jennifer Billock No subject | Jul 2, 2007 11:22 AM | Mail Mess |
| Shannon Rapp No subject | Jul 8, 2007 10:38 AM | Mail Mess |
| Golden Loan Investment No subject | Apr 3, 2009 3:20 AM | Mail Mess |
| Randy Hyde No subject | Oct 13, 2009 9:49 AM | Mail Mess |
| Randy Hyde No subject | Oct 13, 2009 9:49 AM | Mail Mess |
| Lisa Plaski No subject | Apr 8, 2003 2:04 PM | Mail Mess |
| Carrie Kengle No subject | Nov 2, 2002 4:21 PM | Mail Mess |
| Ty-Lör Allen BORING No subject | Aug 11, 2002 12:23 PM | Mail Mess |
| Matty No subject | Jan 29, 2003 7:49 AM | Mail Mess |
| Josh Sparber No subject | Mar 24, 2005 10:54 AM | Mail Mess |
| Lisa Plaski No subject | Jun 1, 2004 6:23 PM | Mail Mess |
| Holly Rhodes No subject | Dec 2, 2004 11:46 AM | Mail Mess |
| Mail Administrator No subject | Nov 30, 2007 8:53 AM | Mail Mess |
| Mail Administrator No subject | Dec 6, 2007 12:27 PM | Mail Mess |
| Mail Administrator No subject | Nov 30, 2007 8:53 AM | Mail Mess |
| Mail Administrator No subject | Dec 6, 2007 12:27 PM | Mail Mess |
| Gale Brown No subject | Apr 6, 2009 11:09 AM | Mail Mess |

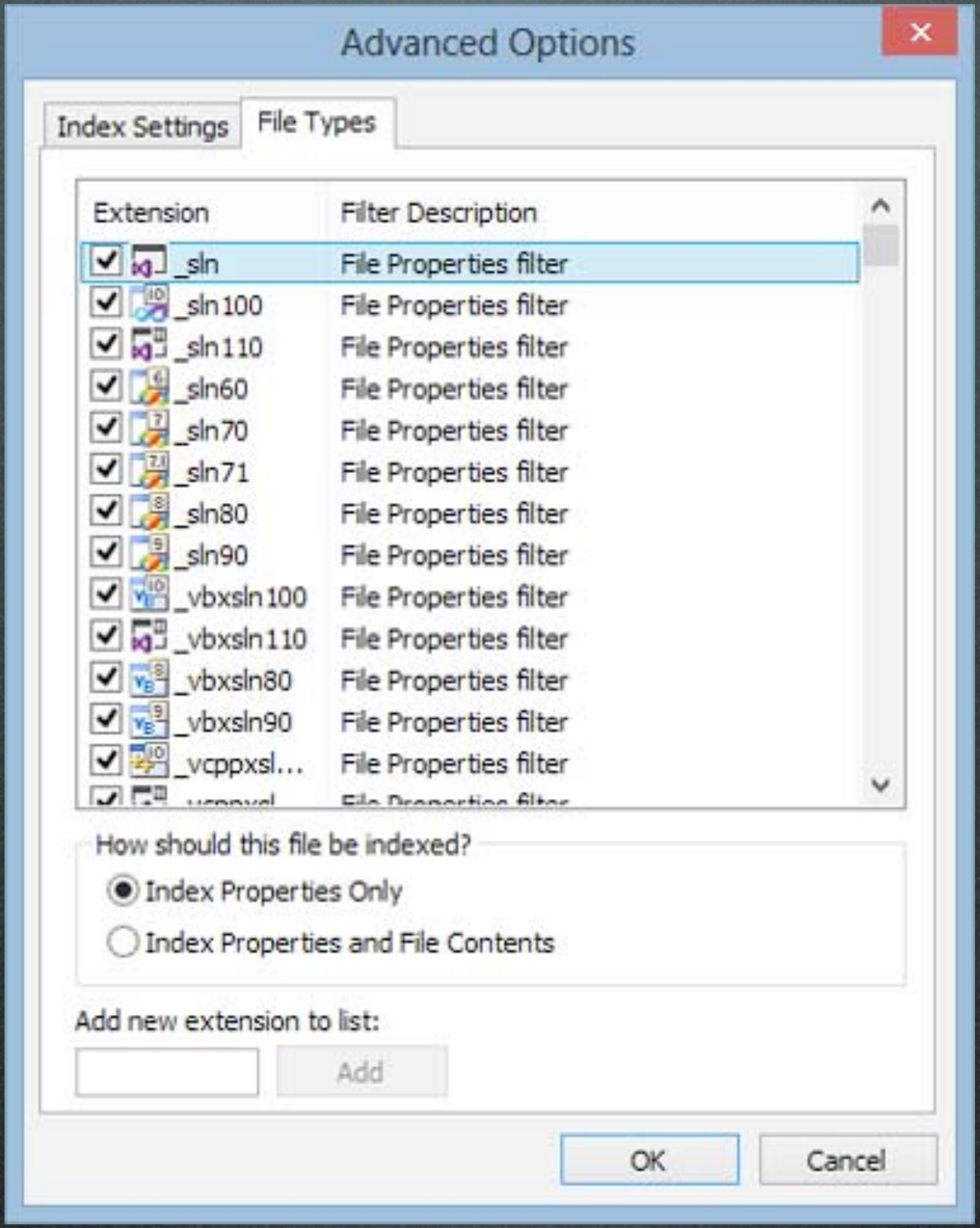
msallin ▸ Do ▸ Ma ▸ Ma ▸ Im ▸ INI ▸ Messages ▸ 53388.emlx

1 selected; more than 10,000 found

Spotlight home

| | |
|---|---|
| | Show All |
| Top Hit | home-01.bmml |
| Definition | noun 1 the place where one… |
| System Preferences | Security |
| Documents | Design Inventory for Creativ… |
| Folders | Hometowns |
| Messages | Knock-knock, matty. 75% Sa… |
| Contacts | honza bernat |
| Events & To Dos | Fancy Pants 2008: The Pants… |
| Images | home.jpg<br>HOME3.jpeg |
| PDF Documents | matty_resume (5).pdf<br>matty_resume (4).pdf |
| Webpages | Michael Jefferson \| LinkedIn<br>People Search Results \| LinkedIn |
| Music | 96 096 ND Nutrition for Kid… |
| Movies | LeavingHome….wmv |
| Fonts | Mini Pics Home Buddies TT …<br>Mini Pics Home Buddies TT … |
| Presentations | Schwab Homepage Design 1…<br>Scanning_Options.pptx |
| | Spotlight Preferences… |

Tuesday, April 5, 2016



Advanced Options

| Extension | Filter Description |
|---|---|
| ☑ _sln | File Properties filter |
| ☑ _sln100 | File Properties filter |
| ☑ _sln110 | File Properties filter |
| ☑ _sln60 | File Properties filter |
| ☑ _sln70 | File Properties filter |
| ☑ _sln71 | File Properties filter |
| ☑ _sln80 | File Properties filter |
| ☑ _sln90 | File Properties filter |
| ☑ _vbxsln100 | File Properties filter |
| ☑ _vbxsln110 | File Properties filter |
| ☑ _vbxsln80 | File Properties filter |
| ☑ _vbxsln90 | File Properties filter |
| ☑ _vcppxsl... | File Properties filter |
| ☑ _vcppxsl | File Properties filter |

How should this file be indexed?

● Index Properties Only

○ Index Properties and File Contents

Add new extension to list:

# The Breach

- Let me count the ways...
  - Social engineering
  - Inside job
  - Lost laptop
  - Less protected (but trusted) law firm

# The Discovery

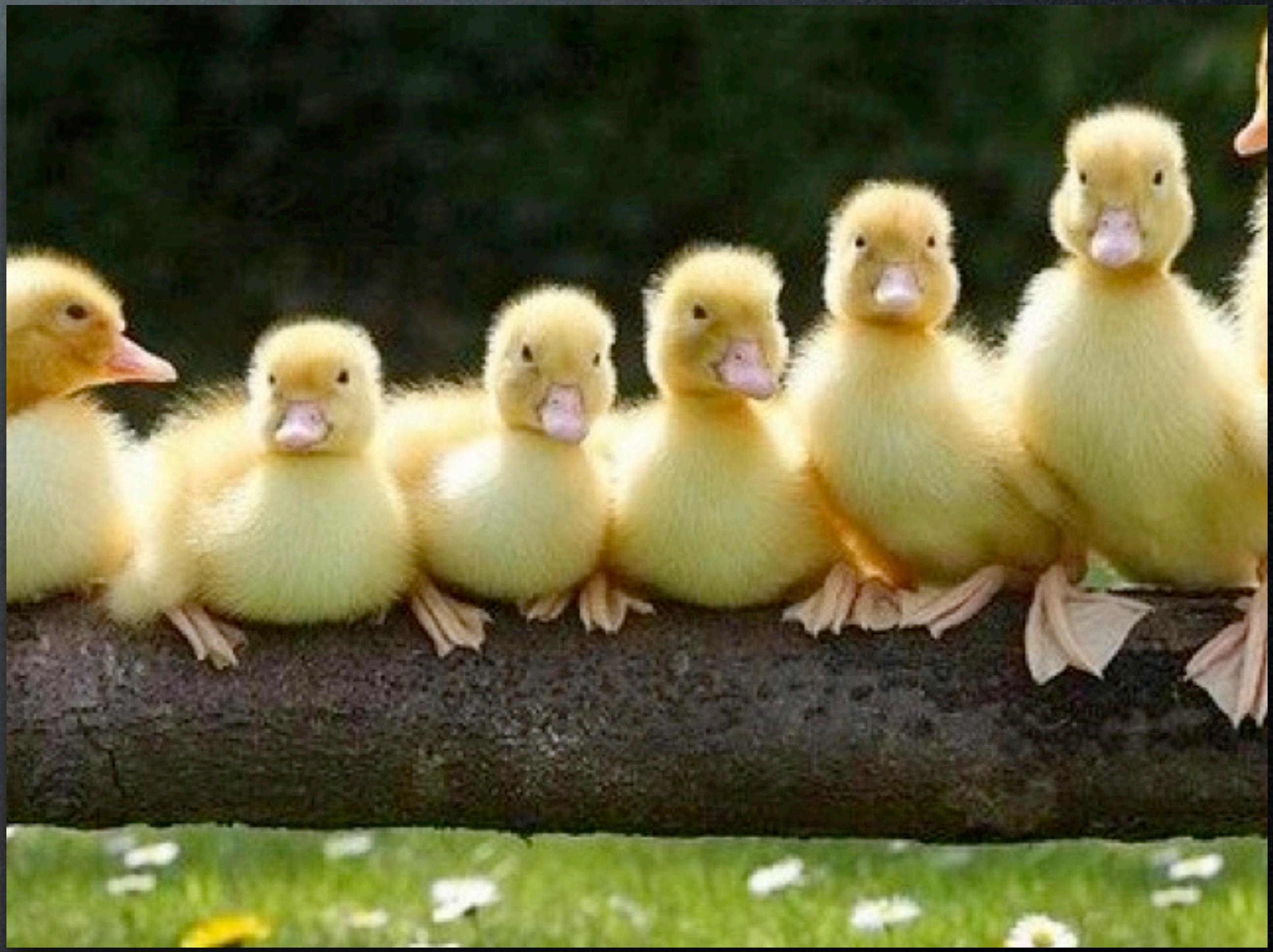
- Need to find it
  - Monitoring
  - Customer complaint
  - Threat email
  - ... (ad nauseam)
- Start the Clock

# The Confession

- You have to help determine...
  - Whom to tell
  - What to tell them
  - When to tell them

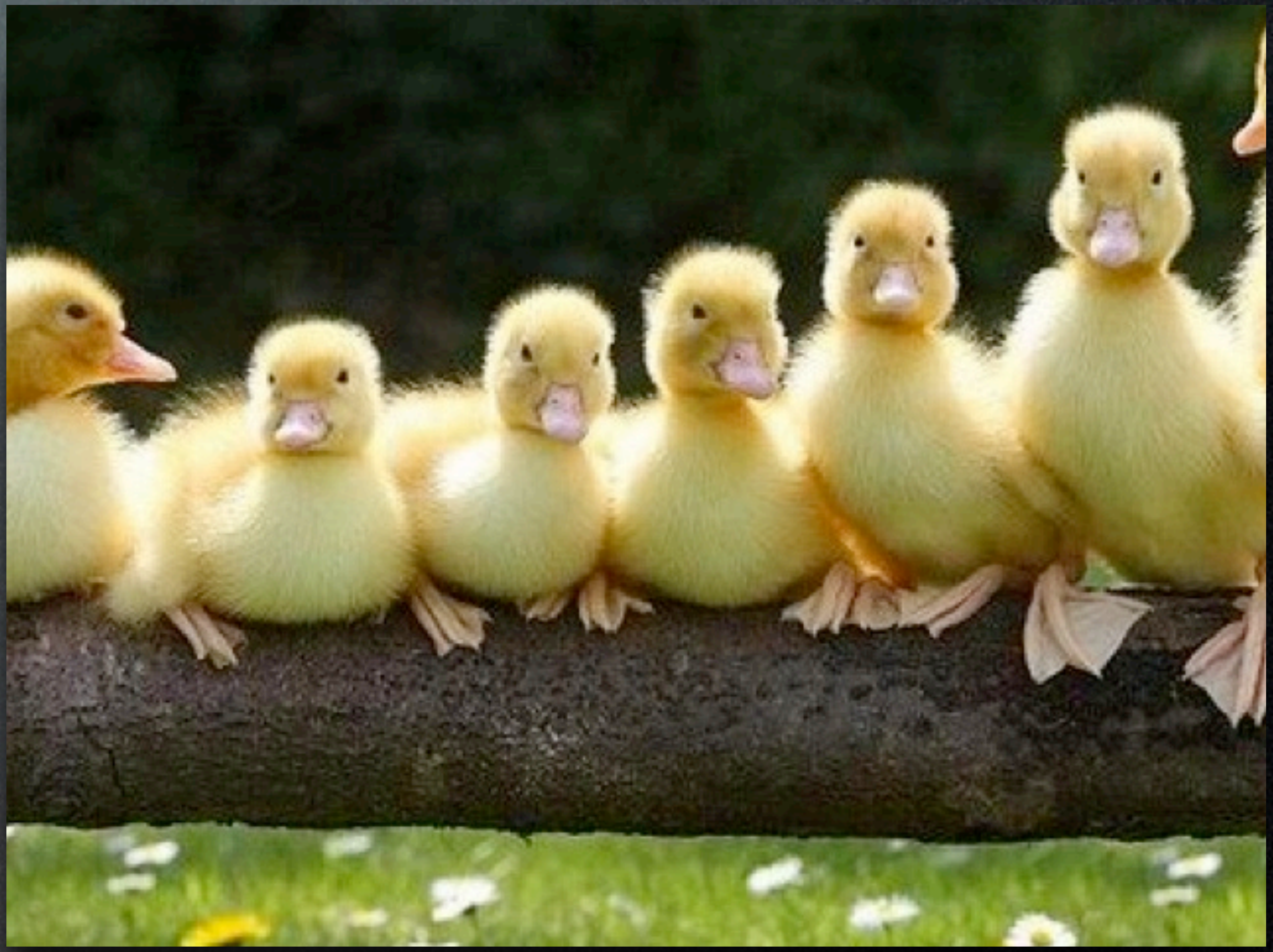
# Timeline

- Activate Response Team
- Call Insurance Agent
- Call the Attorney(s)
- Assign Coordinator
- Preserve the Evidence
- Call Law Enforcement
- Notify Government Agencies*
- Decide Who to Notify
- Offer Credit Monitoring
- Draft Press Release
- Draft FAQ's
- Notify Credit Card Companies



# Timeline

- Activate Response Team
- Call Insurance Agent
- Call the Attorney(s)
- Assign Coordinator
- Preserve the Evidence
- Call Law Enforcement
- Notify Government Agencies*
- Decide Who to Notify
- Offer Credit Monitoring
- Draft Press Release
- Draft FAQ's
- Notify Credit Card Companies



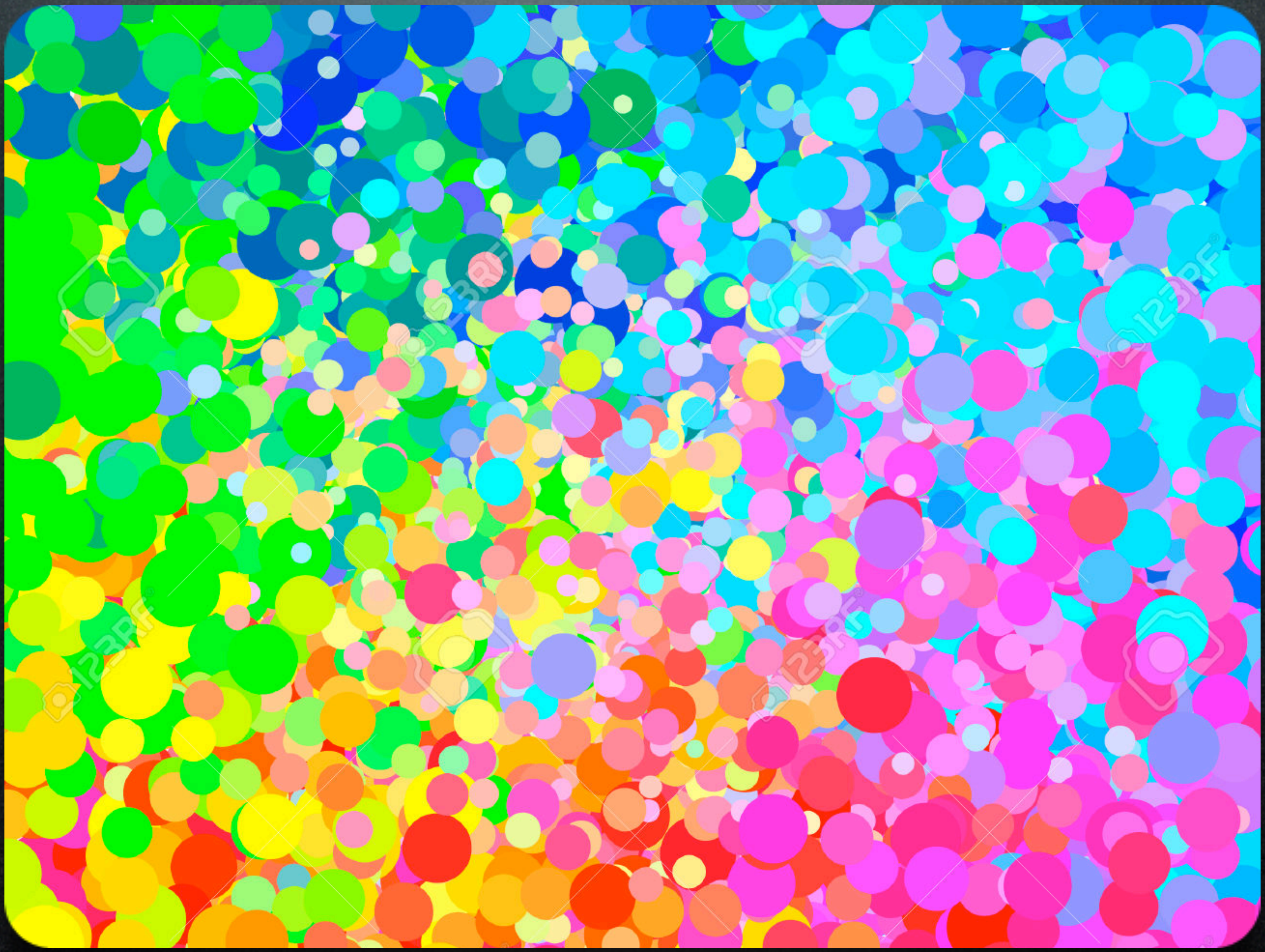
# The Clock is Ticking...

- Lots of laws (may) apply
- Some have short fuses
- You have to find out which states are affected
- You have to find out what kind of data was accessed or copied

# What the law should be

# But the Feds...

... and so the states...



...gave us a mishmash

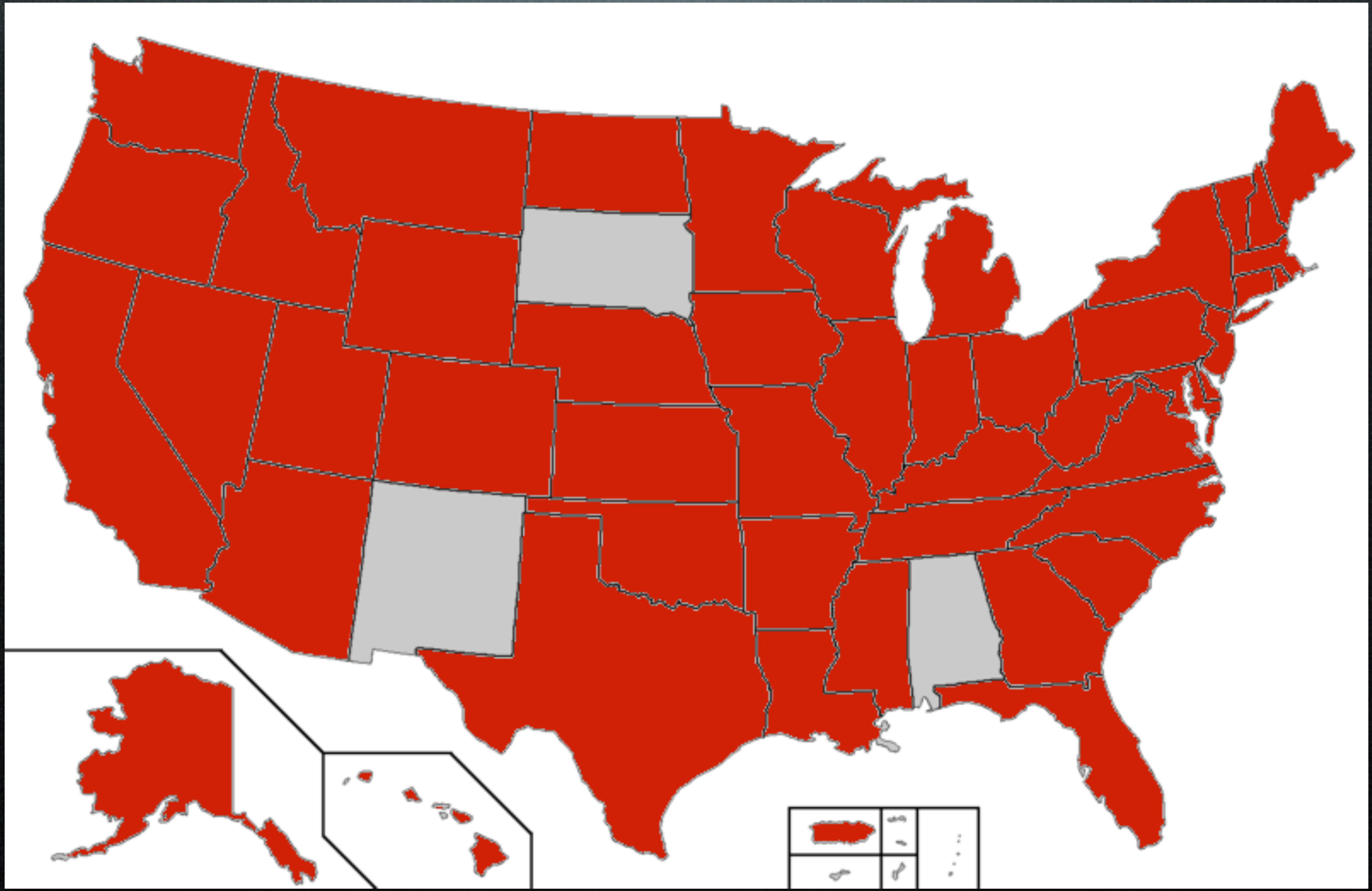
# Oliver Wendell Holmes

- The young man knows the rules...
- ... but the old man knows the exceptions

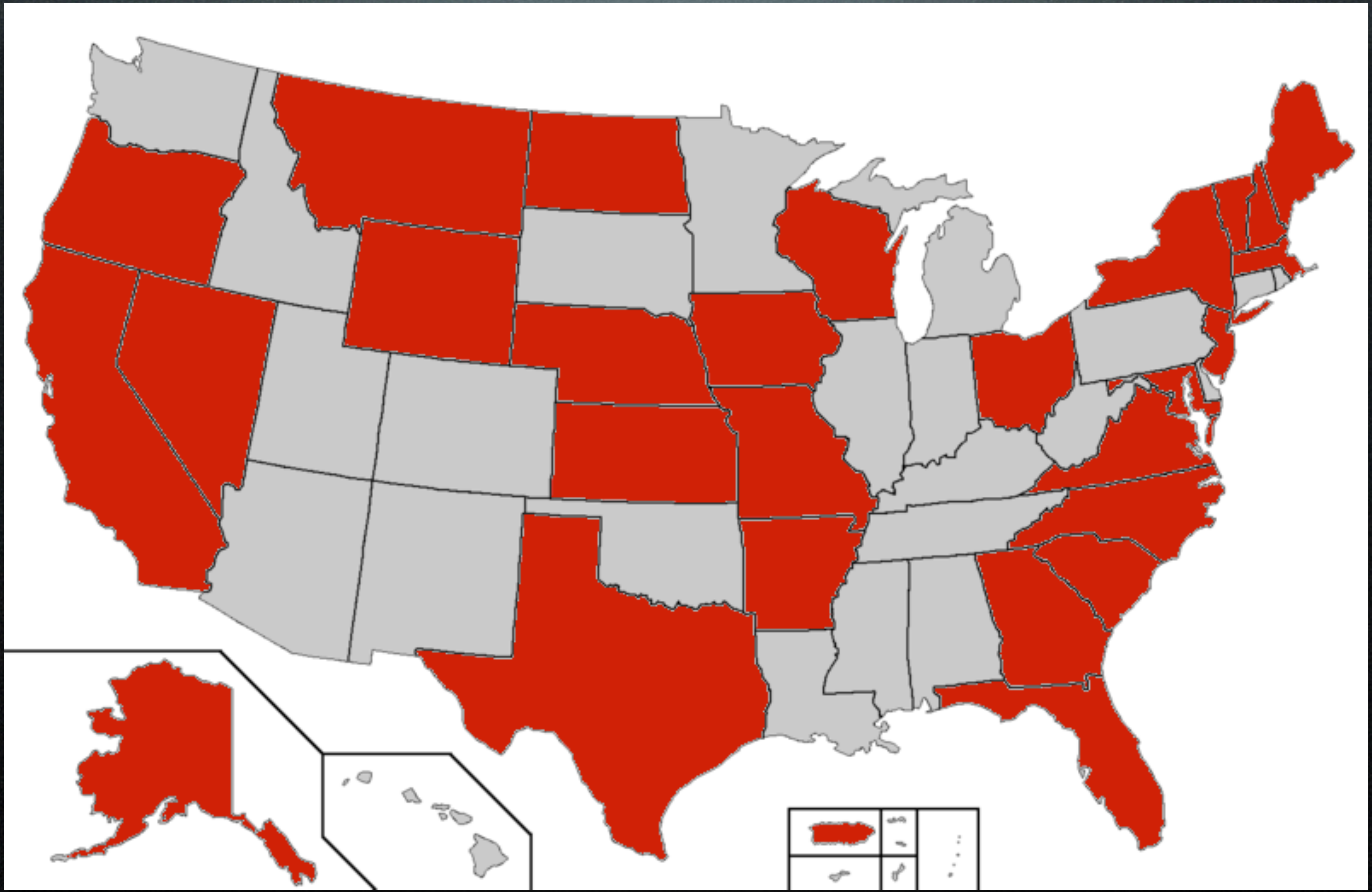
# The Rules

- Personal Information
    - Common elements (First Name, Last Name, Gov’t ID, Bank #, etc.)
- Breach of Security
    - The unlawful and unauthorized acquisition of personal information that compromises its security, confidentiality or integrity

# The Exceptions



# Safe Harbor for Encryption



Broader definition of "Personal Information"

# Broader Definitions

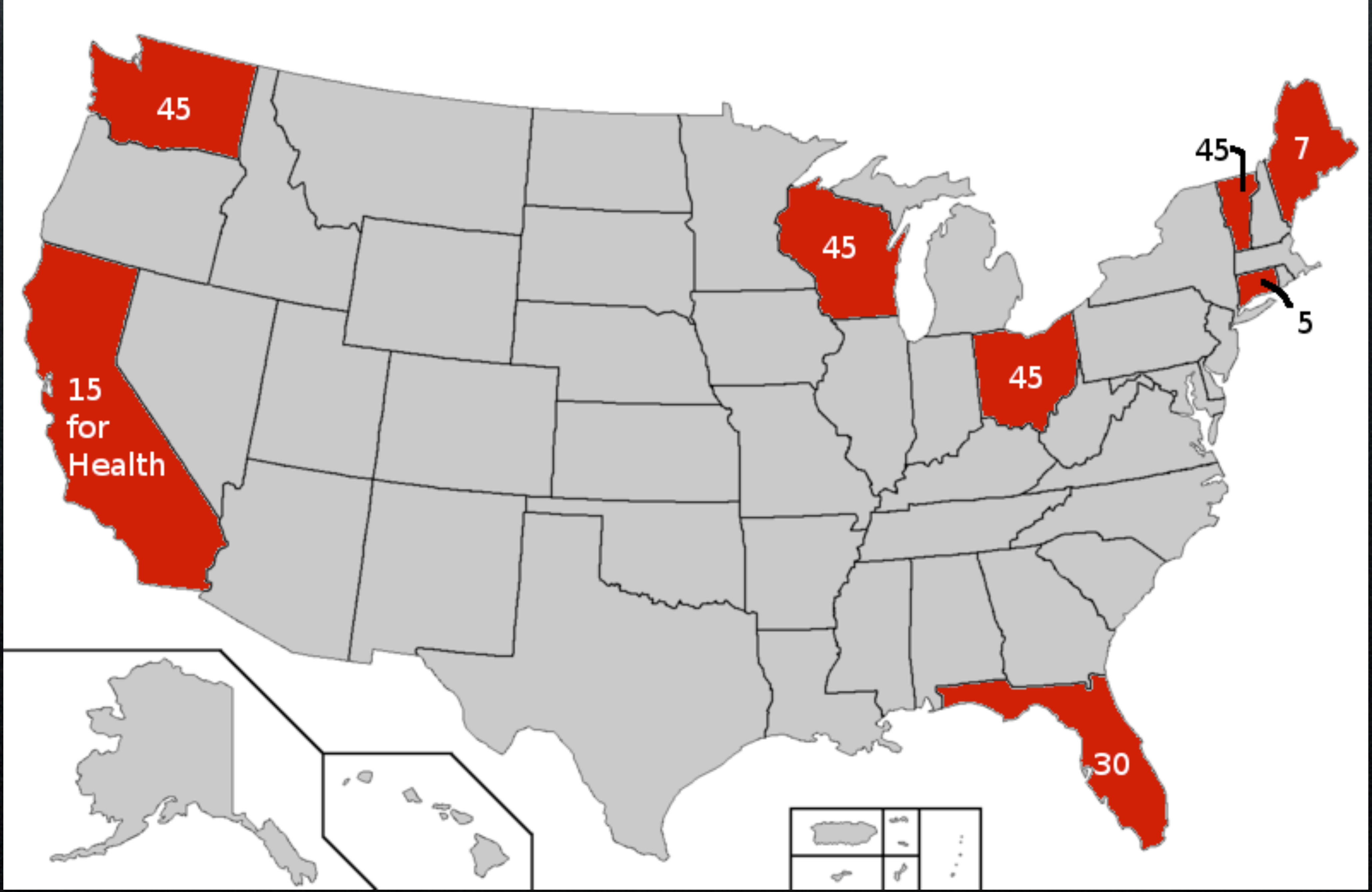
- Passwords to online accounts (CA, NV) (But NC expressly excludes)
- Taxpayer ID (MD, MT)
- Passwords to financial accounts (AK, FL, GA, IA, KS, ME, MA, MO, NY, ND, OR, SC, VT, WY, D.C., PR)

# Broader Definitions

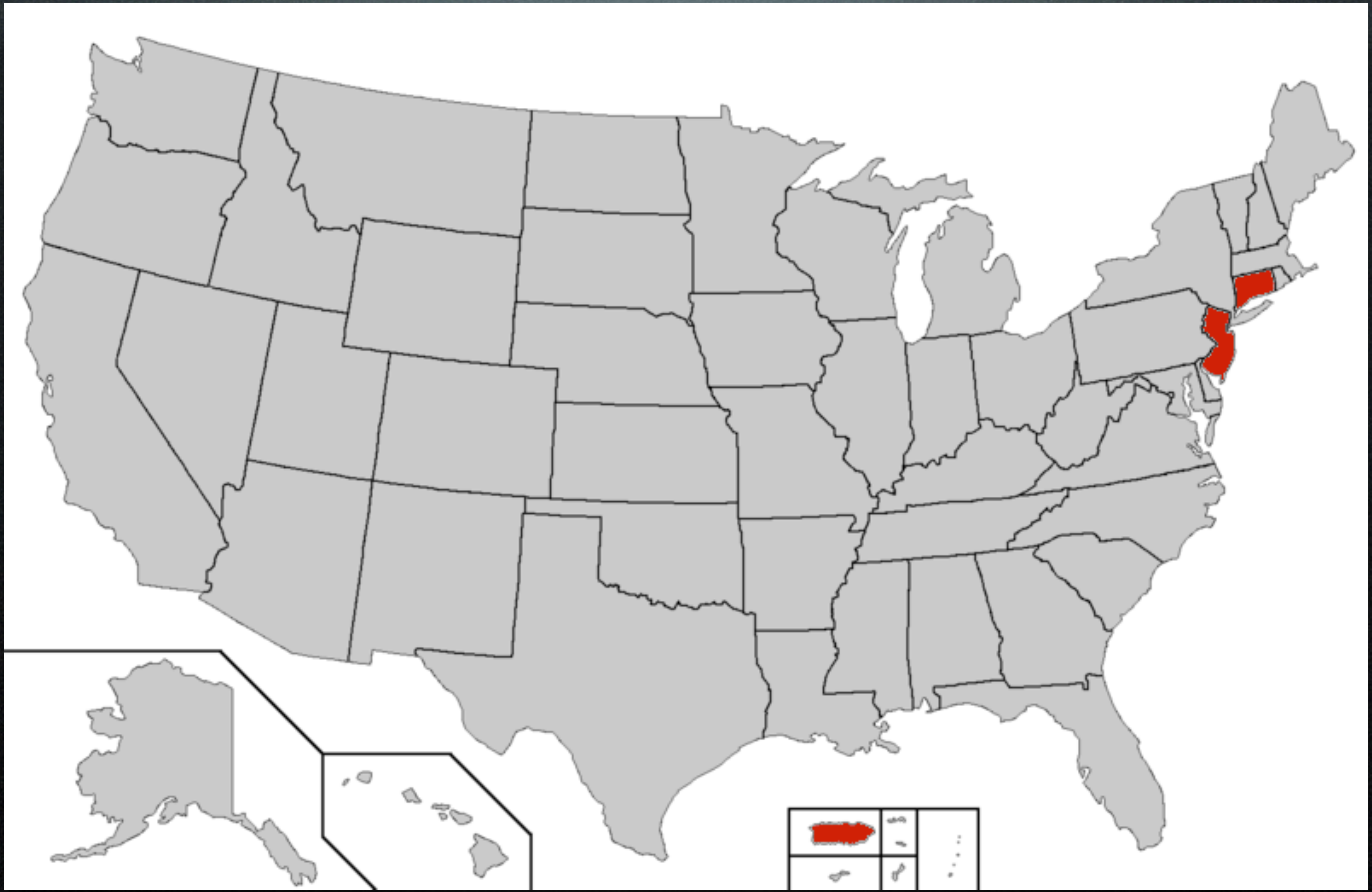
- Financial account info - with or without password (MA)
- Dissociated data -- if linked (NJ)
- Biometric data (NE, NC, VA)
- Digital/Electronic signature (ND)

# Broader Definitions

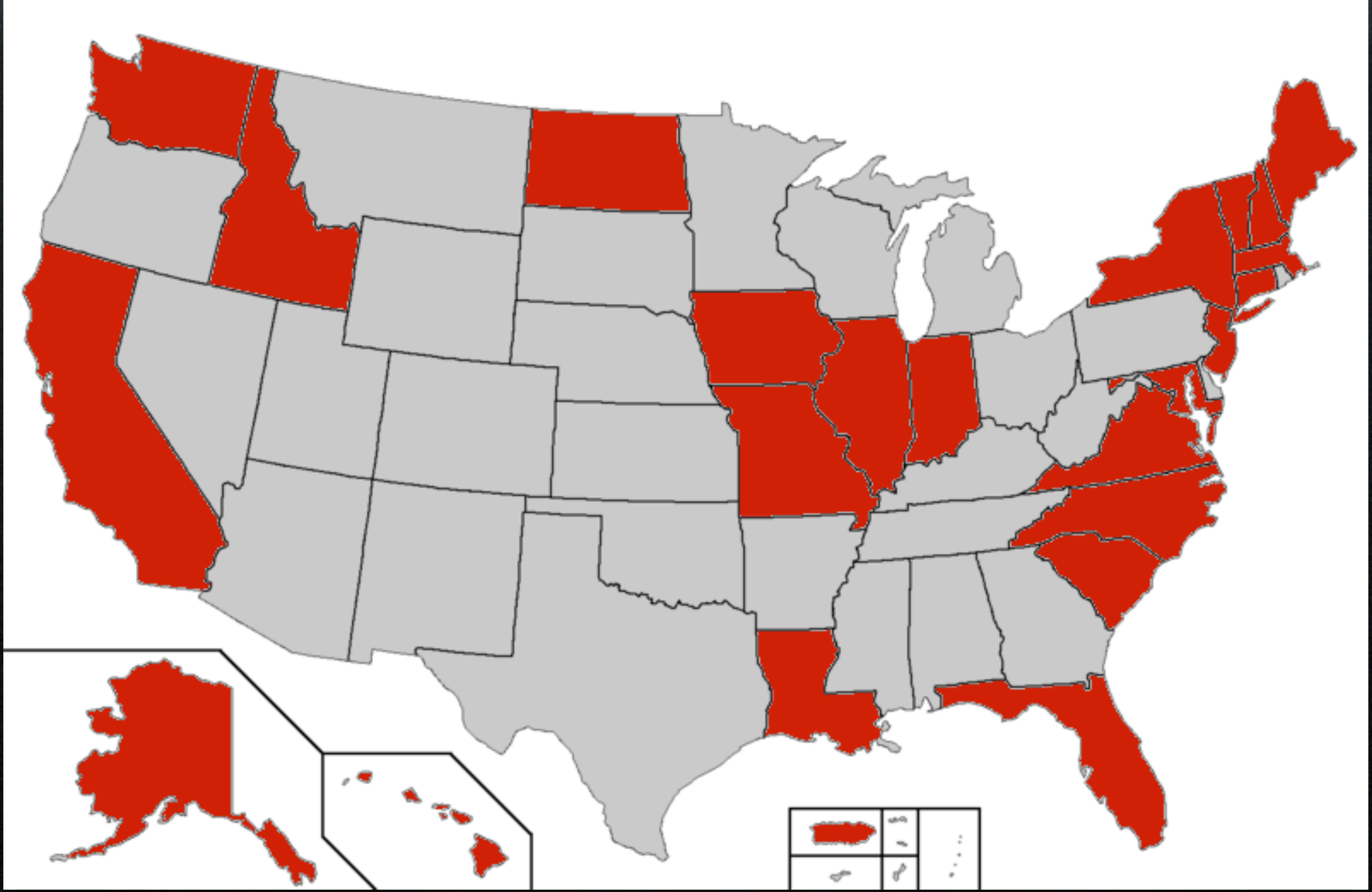
- Health ID for med account (NV, WY)
- Medical information & history (AR, CA, FL, MO, MT, NH, ND, TX, VA, WI (DNA only), WY, PR)



# Short-fuse Timing for Notification



# Trigger on Access (not Acquisition)



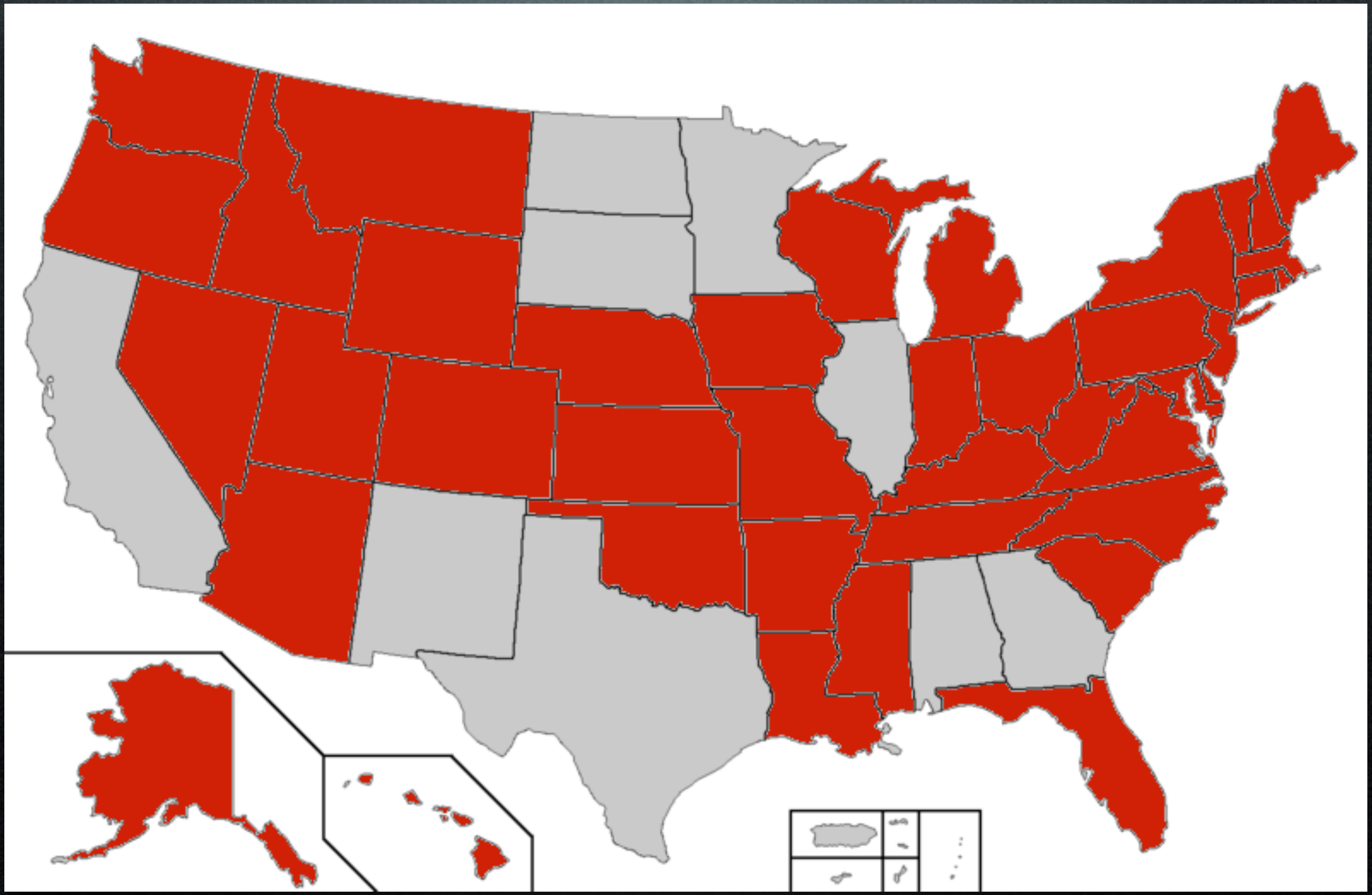
# Notify the Attorney General or State Agency

# Notify the State Gov’t.

- Notify government if X customers are to be notified.
  - 1 or more - CT, IN, LA, MD, MA, MO, MT, NH, NJ, NY, NC, PR, VT
  - 250 or more - ND
  - 500 or more - CA, FL, IA, WA
  - 1000 or more - HI, MO, SC, VA

# Notify the State Gov't.

- Notify government if its agency was breached. (ID, IL)
- Notify government if the entity is governed by a professional or financial regulatory agency. (ME)
- Notify government that no notice required. (AK)



# Risk of Harm Analysis

# Risk of Harm Analysis

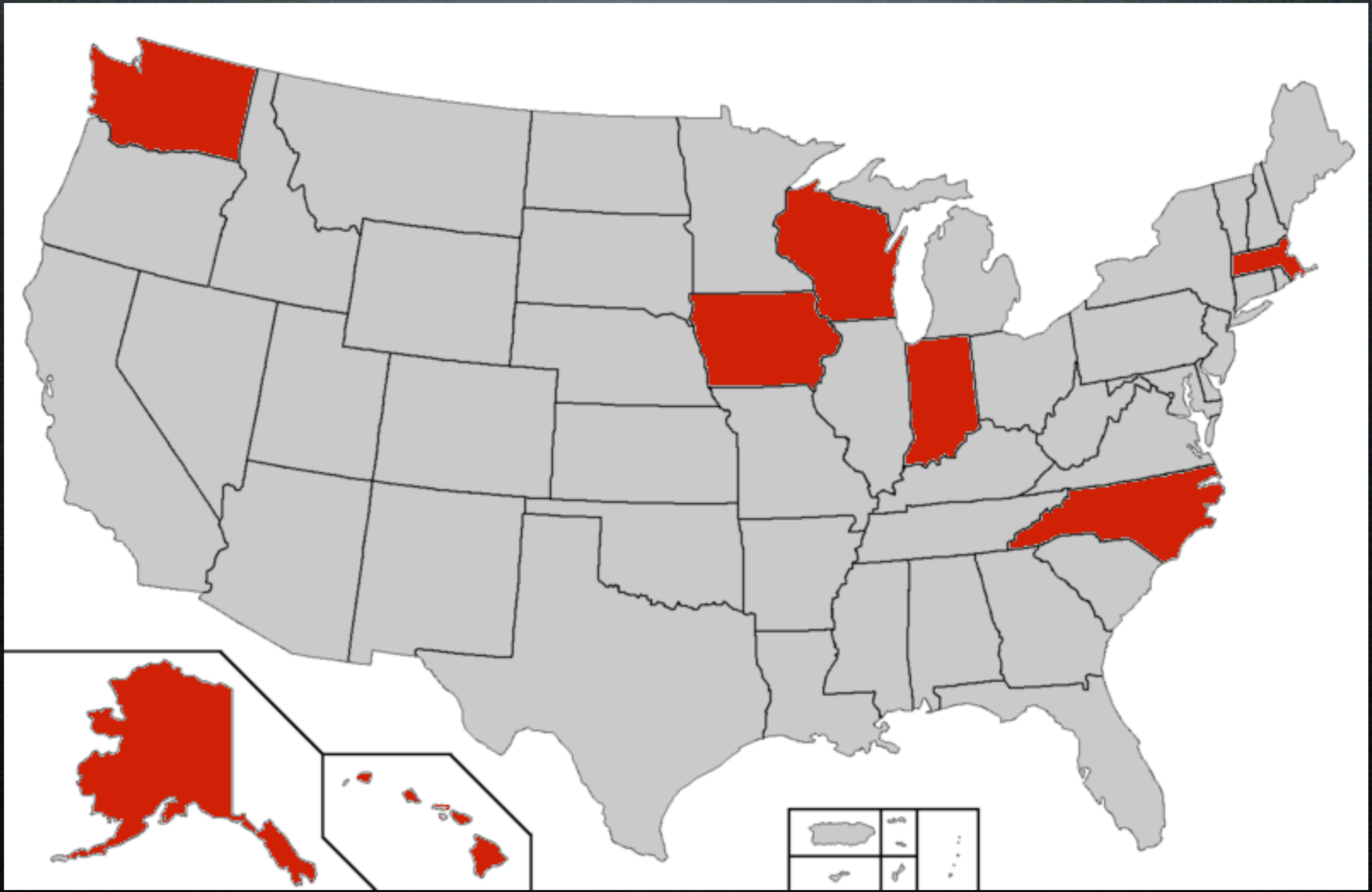
- Have to determine whether there was or is a reasonable likelihood that harm to the consumer has or will result. (AK, AR, CO, CT, DE, HI, ID*, IN, IA, KS, KY, LA, ME, MS, MO, NE, NC, OH, OK, OR, RI, SC, WA)
- Have to determine if there was material compromise (AZ, ID*, MT, NV, PA, TN, WI, WY)

# Risk of Harm Analysis

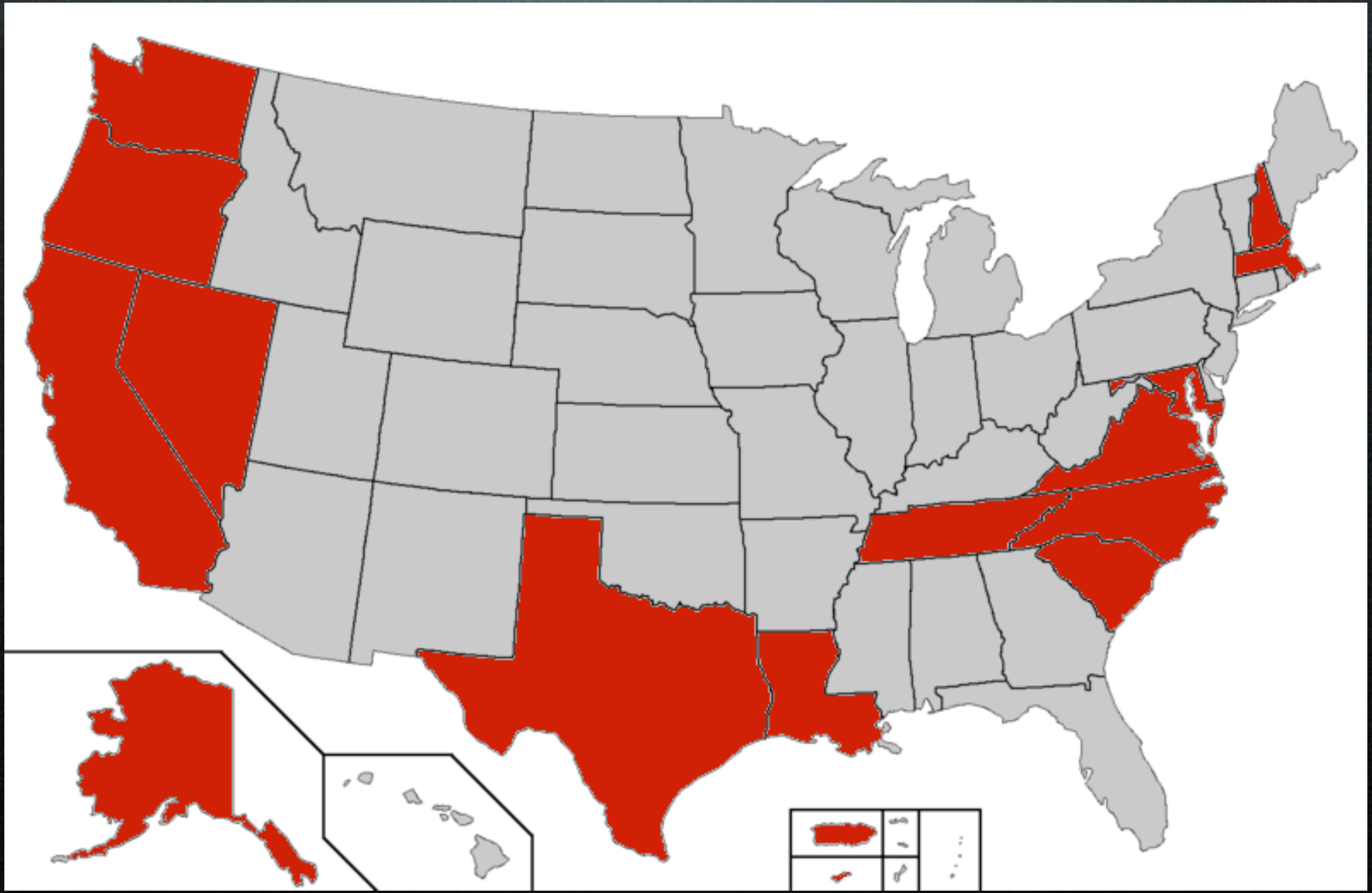
- Have to determine if the PI was not and will not be misused as a result of the breach. (MD)
- Have to determine if there is a substantial risk of identity theft (MA)
- Have to determine if the breach has or is likely (or will) to cause substantial loss or injury. (MI, VA, WV)

# Risk of Harm Analysis

- Must determine if there was no misuse of data and not reasonably likely to occur. (NH, UT)
- Must determine if misuse is not reasonably possible. (NJ, VT)
- Must determine if there are “indications” of misuse. (NY)



# Paper included in Breach Rubric



# Private Cause of Action Permitted

# Private Cause of Action

- Litigation Hold Notice must be imposed
  - In addition to law enforcement effort
  - Includes policies/procedures/audits
  - Emails, server logs
  - ...

# Private Cause of Action

- DR 1.05 violation?
- Malpractice?
- Clients seeking indemnification from the firm that "allowed" or facilitated the breach?
- Law firm as scapegoat?

# Federal Laws

- FTC Act
- Securities
- CFAA
- GLBA
- HIPAA
- COPPA
- Many more...

And lets not forget...

# What to Expect

- IT will have to find answers QUICKLY

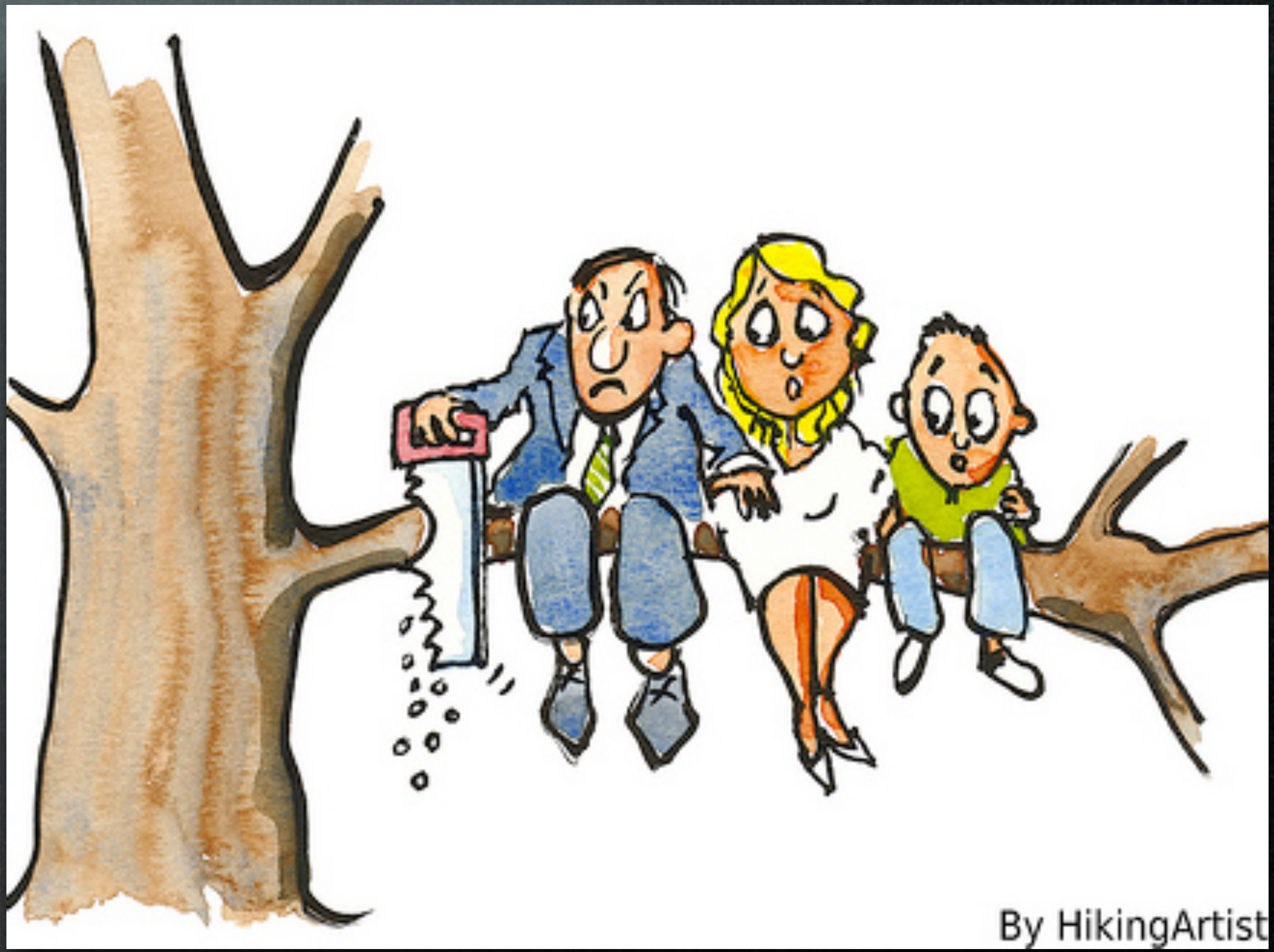
- You will need to make a distinction between access and acquisition

- You will need to supply a full list of what data types were compromised

- You will have a short fuse

# The Consequences

- Exposure to losses
- Lost sales/reputation
- FTC Action for Violations of Privacy Policy
- 20 years of IT auditing
- Disclosure in SEC 8-K and/or 10-K filings


By HikingArtist

# The Aftermath

- In the past, there were few consequences
- Not so today
- This can get a CEO fired
- Future board members likely to have IT expertise

# Conclusions

- Watch what the FTC and NIST defines as "reasonable"
- Active monitoring
- Use encryption
- Compartmentalize
- Rethink indexing
- Have a plan ready in case you have a short fuse on notification

# Questions?

Ronald Chichester, JD, CISA

713-302-1679

Ron@TexasComputerLaw.com