CyberSecurity Legislation

Ronald L. Chichester, Esq.
Ronald Chichester, P.C.
www.texascomputerlaw.com

Presented to the State Bar Annual Meeting
in Dallas, Texas
on June 20, 2013

Overview

Overview

CyberSecurity

Overview

CyberSecurity

CFAA

Overview

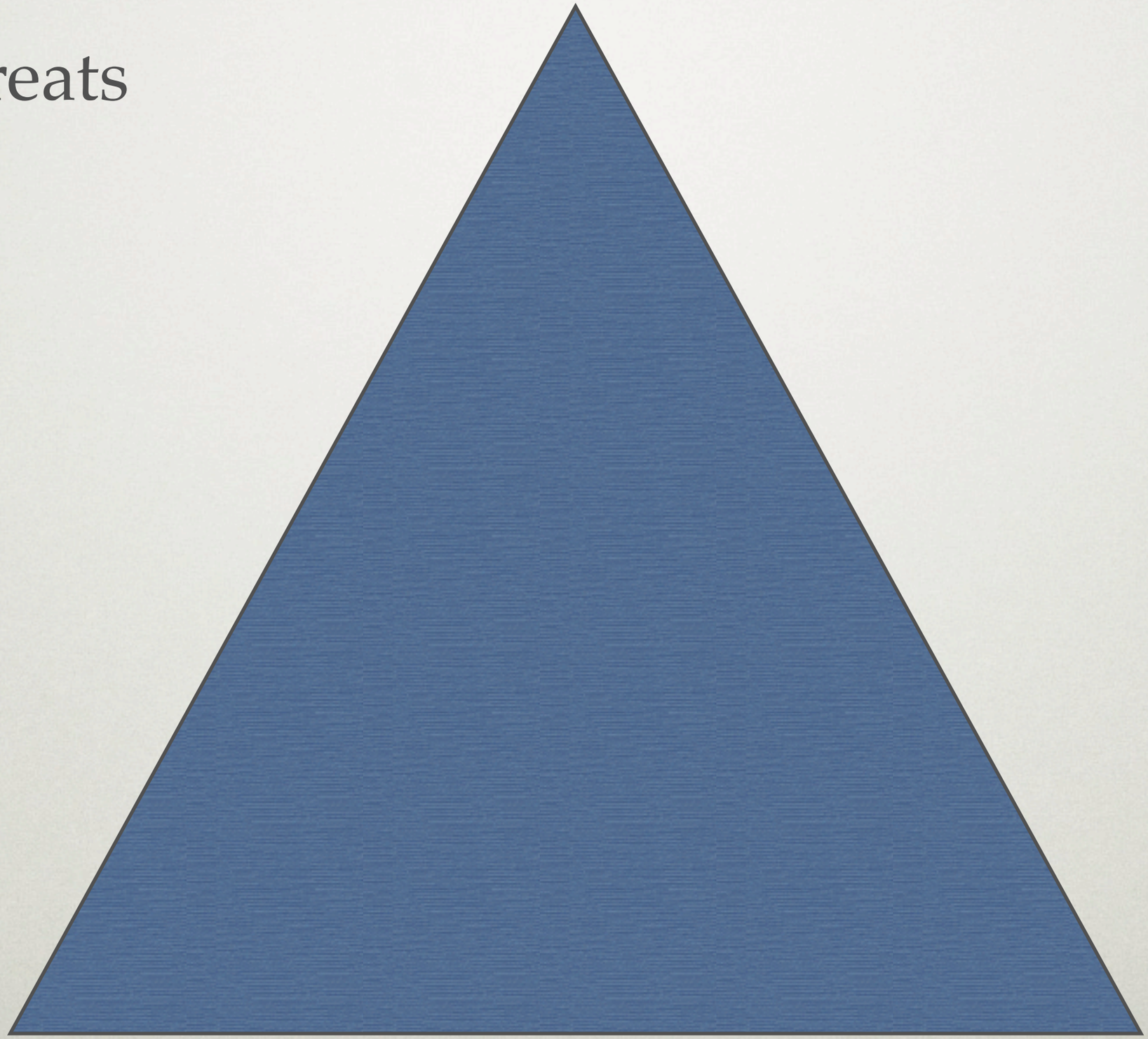
CyberSecurity

CFAA

Seizure & Forfeiture

CyberSecurity

The Threats



The Threats

The Threats


Sophisticated
Threat Actors
Opportunistic Threat Actors

The Threats


ATA
Sophisticated Threat Actors
Opportunistic Threat Actors

The "Other" Current Situation

The "Other" Current Situation

- Designer worms and malware are prevalent

The "Other" Current Situation

- Designer worms and malware are prevalent
- Designer botnets already attacking

The "Other" Current Situation

- Designer worms and malware are prevalent
- Designer botnets already attacking
- Desktop war is lost

The "Other" Current Situation

- Designer worms and malware are prevalent
- Designer botnets already attacking
- Desktop war is lost
- Smartphone war is in progress

The "Other" Current Situation

- Designer worms and malware are prevalent
- Designer botnets already attacking
- Desktop war is lost
- Smartphone war is in progress
- Employment trends add to pressure

The Current Situation

The Current Situation

- Most businesses require Internet access for critical operations & e-commerce

The Current Situation

- Most businesses require Internet access for critical operations & e-commerce
- Prevalence of Flame, Stuxnet & progeny illustrate inadequacy of corporate and government defenses

The Current Situation

- Most businesses require Internet access for critical operations & e-commerce
- Prevalence of Flame, Stuxnet & progeny illustrate inadequacy of corporate and government defenses
- Government has concluded that US is vulnerable to cyberwarfare

Legislative Trends

Legislative Trends

- To reduce vulnerability to cyberwarfare, government concluded that regulation of the Internet is necessary

Legislative Trends

- To reduce vulnerability to cyberwarfare, government concluded that regulation of the Internet is necessary
- Dilemma: Gov't doesn't own the 'Net

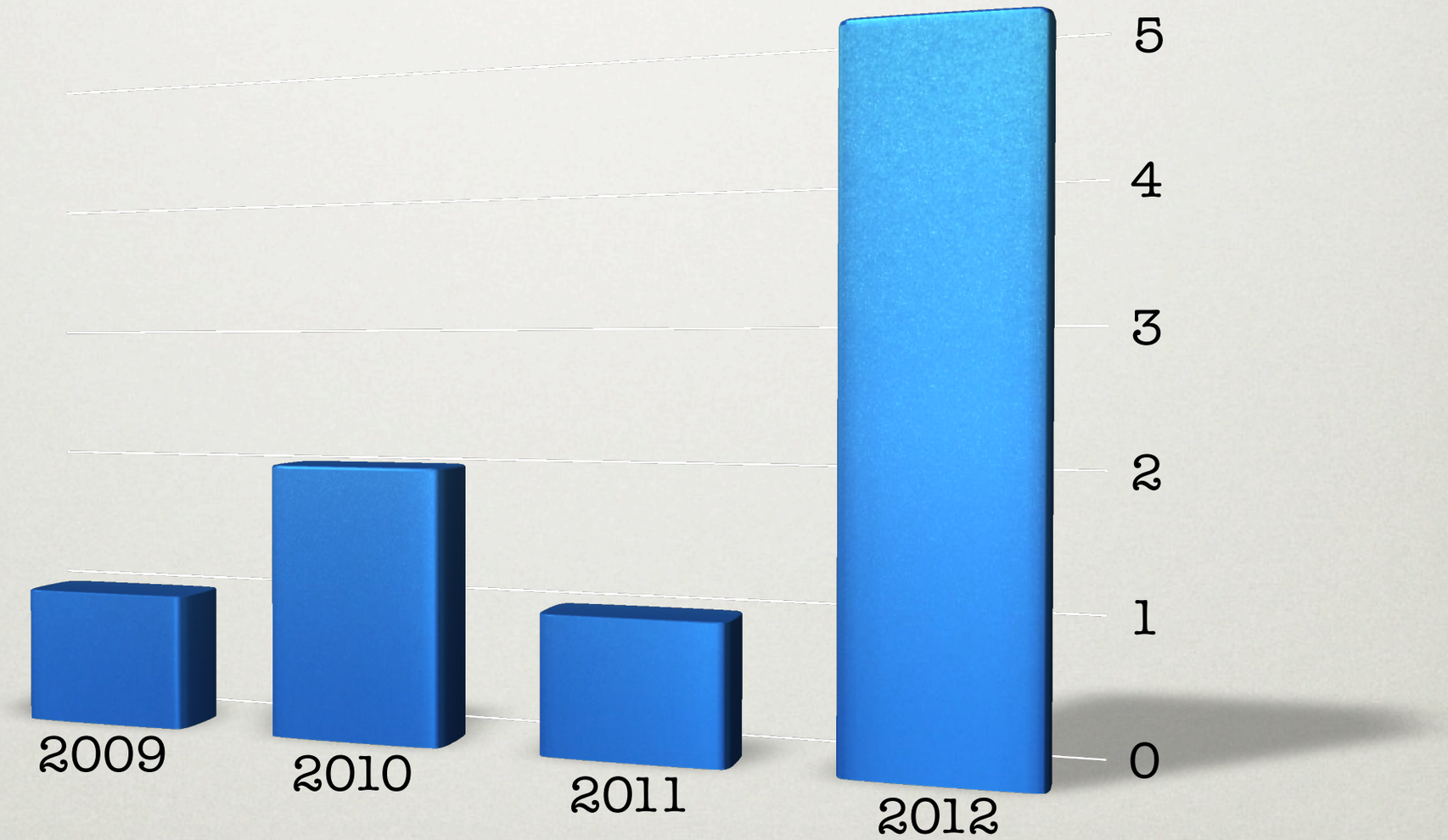
Legislative Trends

- To reduce vulnerability to cyberwarfare, government concluded that regulation of the Internet is necessary
- Dilemma: Gov't doesn't own the 'Net
- Solution: Regulation

Legislative Trends

- To reduce vulnerability to cyberwarfare, government concluded that regulation of the Internet is necessary
- Dilemma: Gov't doesn't own the 'Net
- Solution: Regulation
- Legislation working to control Internet activities through corporations

CyberSecurity Bills



2013 CybeSecurity Bills

- CISPA
- CyberSecurity Act of 2013
- SOPA / PIPA (?)
- CFAA

Cyber Intelligence Sharing and Protection

Cyber Intelligence Sharing and Protection

- CISPA for short

Cyber Intelligence Sharing and Protection

- CISPA for short
- Same story as in 2012...

Cyber Intelligence Sharing and Protection

- CISPA for short
- Same story as in 2012...
- Passed the House

Cyber Intelligence Sharing and Protection

- CISPA for short
- Same story as in 2012...
- Passed the House
- President threatened to Veto

Cyber Intelligence Sharing and Protection

- CISPA for short
- Same story as in 2012...
- Passed the House
- President threatened to Veto
- Died in the Senate

Cyber Intelligence Sharing and Protection

- CISPA for short
- Same story as in 2012...
  - Passed the House
  - President threatened to Veto
  - Died in the Senate
  - Dems wanted “mandatory security standards for critical infrastructure”

CyberSecurity Act Legislative Trends

CyberSecurity Act Legislative Trends

- Progress so far...

CyberSecurity Act Legislative Trends

- Progress so far...
  - Internet “kill switch” off the table

CyberSecurity Act Legislative Trends

- Progress so far...
  - Internet “kill switch” off the table
  - First President was, then Congress was, now DHS might promulgate the regulations

CyberSecurity Act Legislative Trends

- Progress so far...
  - Internet "kill switch" off the table
  - First President was, then Congress was, now DHS might promulgate the regulations
  - Expect limited ability to stop your designation as "critical infrastructure"

Upcoming Obligations

Upcoming Obligations

- Planning & Infrastructure

Upcoming Obligations

- **Planning & Infrastructure**
  - Probably through Executive Branch

Upcoming Obligations

- **Planning & Infrastructure**
  - Probably through Executive Branch
- **Certifications**

Upcoming Obligations

- **Planning & Infrastructure**
  - Probably through Executive Branch
- **Certifications**
  - Promulgated by DHS via CFR

Upcoming Obligations

- **Planning & Infrastructure**
  - Probably through Executive Branch
- **Certifications**
  - Promulgated by DHS via CFR
- **Enforcement**

Upcoming Obligations

- **Planning & Infrastructure**
  - Probably through Executive Branch
- **Certifications**
  - Promulgated by DHS via CFR
- **Enforcement**
  - Loss of Certification = No Internet

An Example

2011

SEC Disclosure Guidelines

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

SEC Guidelines

SEC Guidelines

- Affects publicly traded companies

SEC Guidelines

- Affects publicly traded companies
- Must disclose cybersecurity risks...

SEC Guidelines

- Affects publicly traded companies
- Must disclose cybersecurity risks...
- ... and cybersecurity incidents...

SEC Guidelines

- Affects publicly traded companies
- Must disclose cybersecurity risks...
- ... and cybersecurity incidents...
- ... that investors would consider important to an investment decision

SEC Guidelines

- Affects publicly traded companies
- Must disclose cybersecurity risks...
- ... and cybersecurity incidents...
- ... that investors would consider important to an investment decision
- May need to file reports on Form 6-K or 8-K for costs/consequences of incidents

More Risk

More Risk

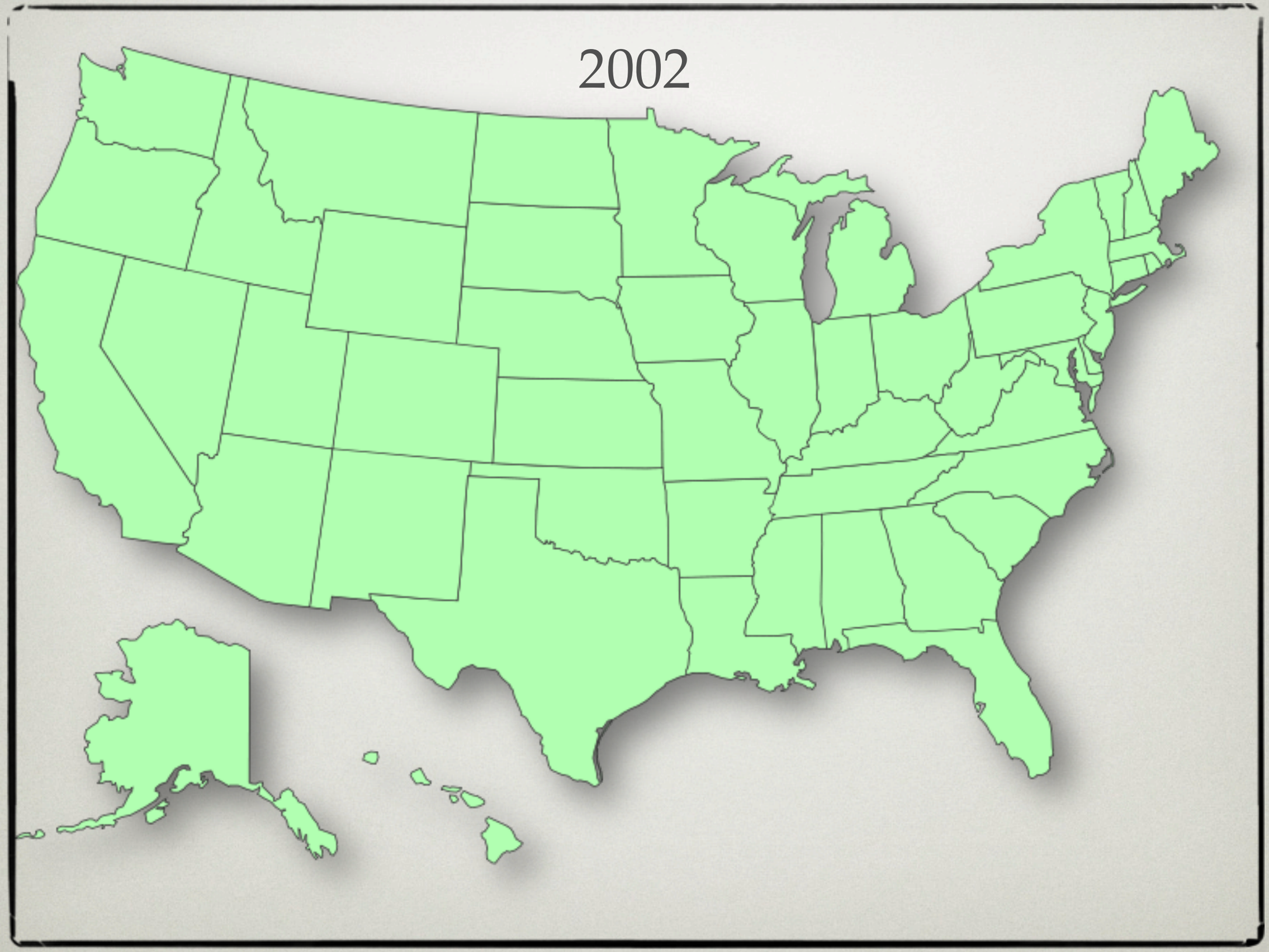
More Enforcement

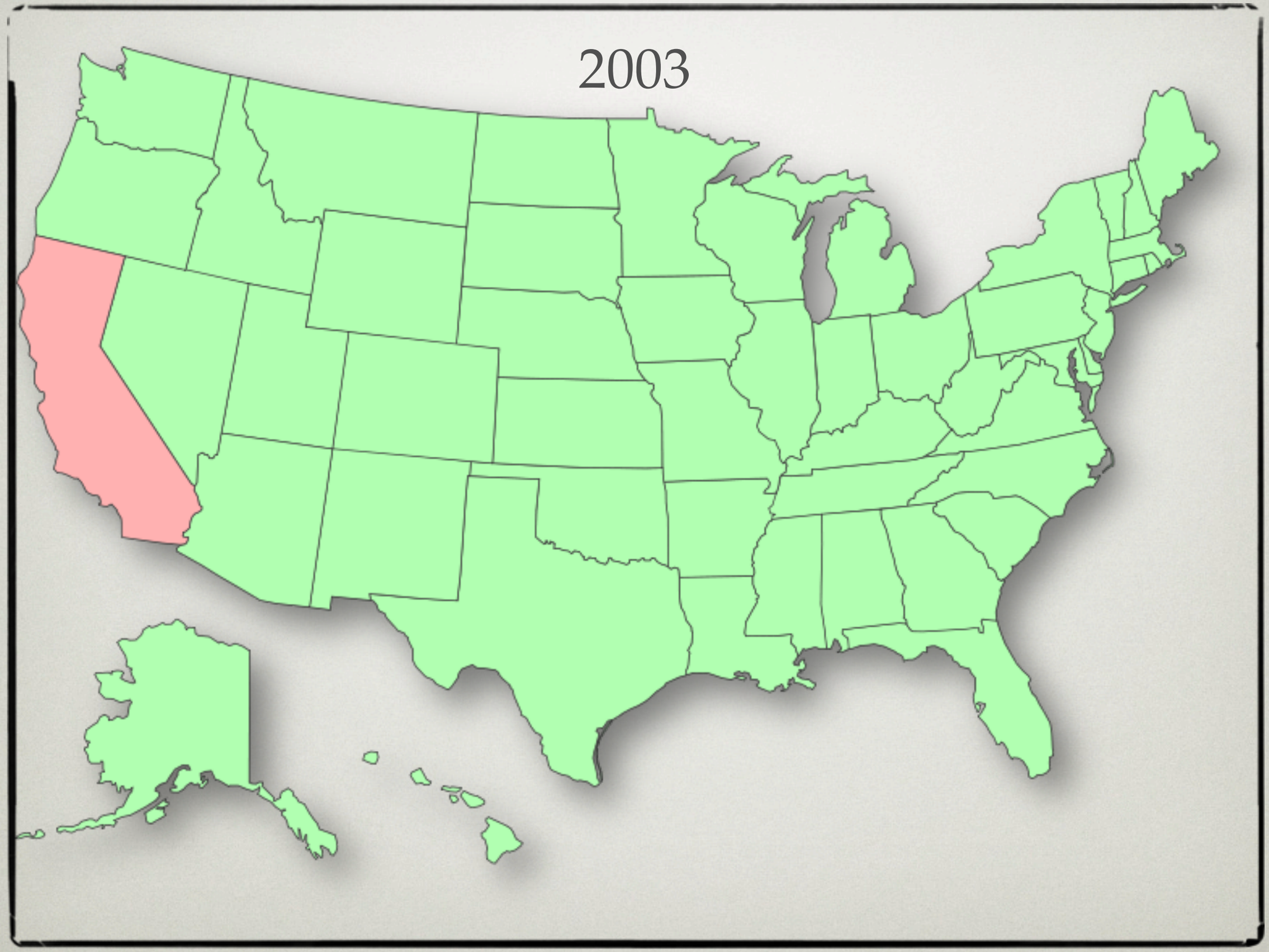
Another Example:

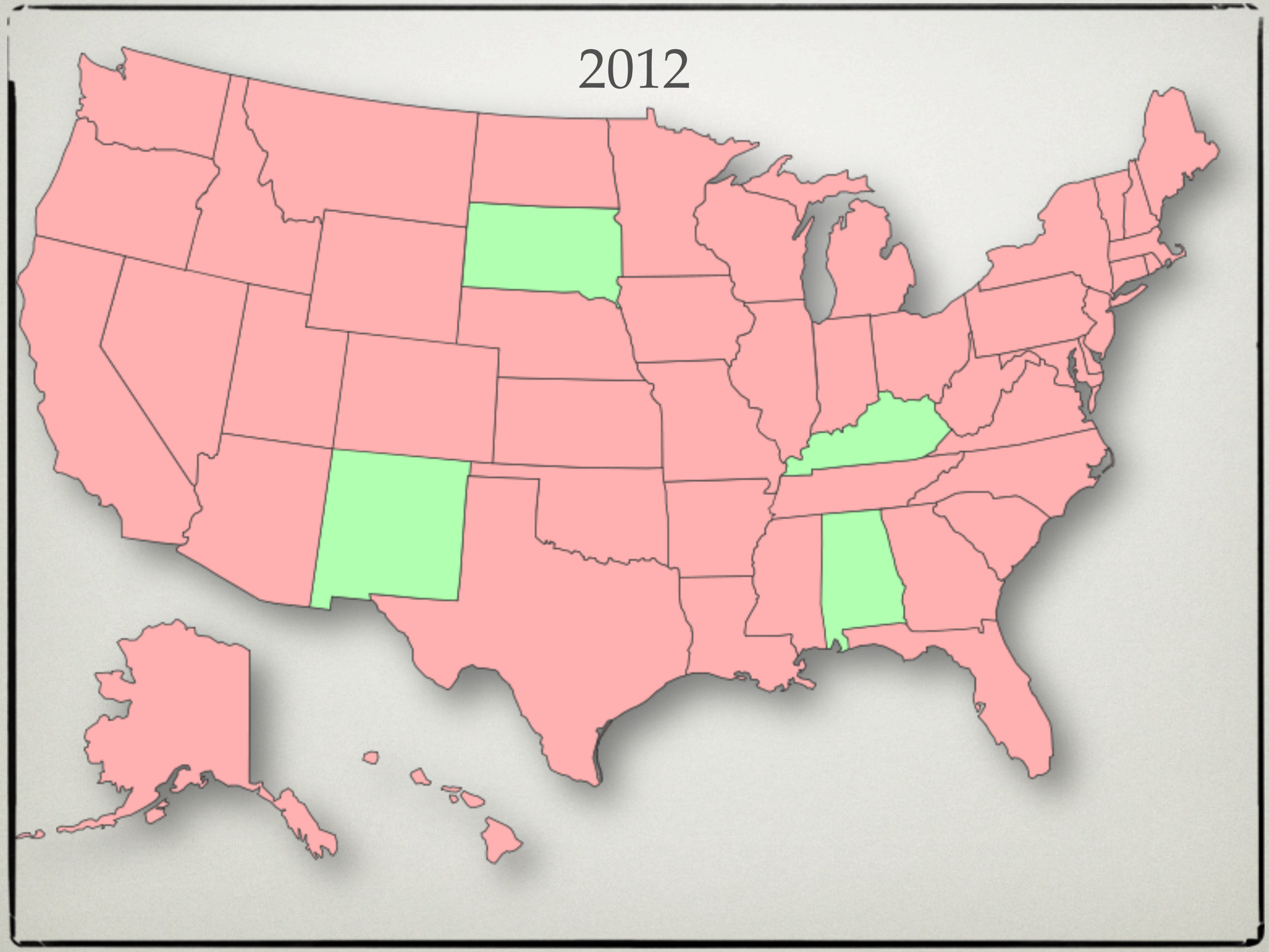
Another Example:

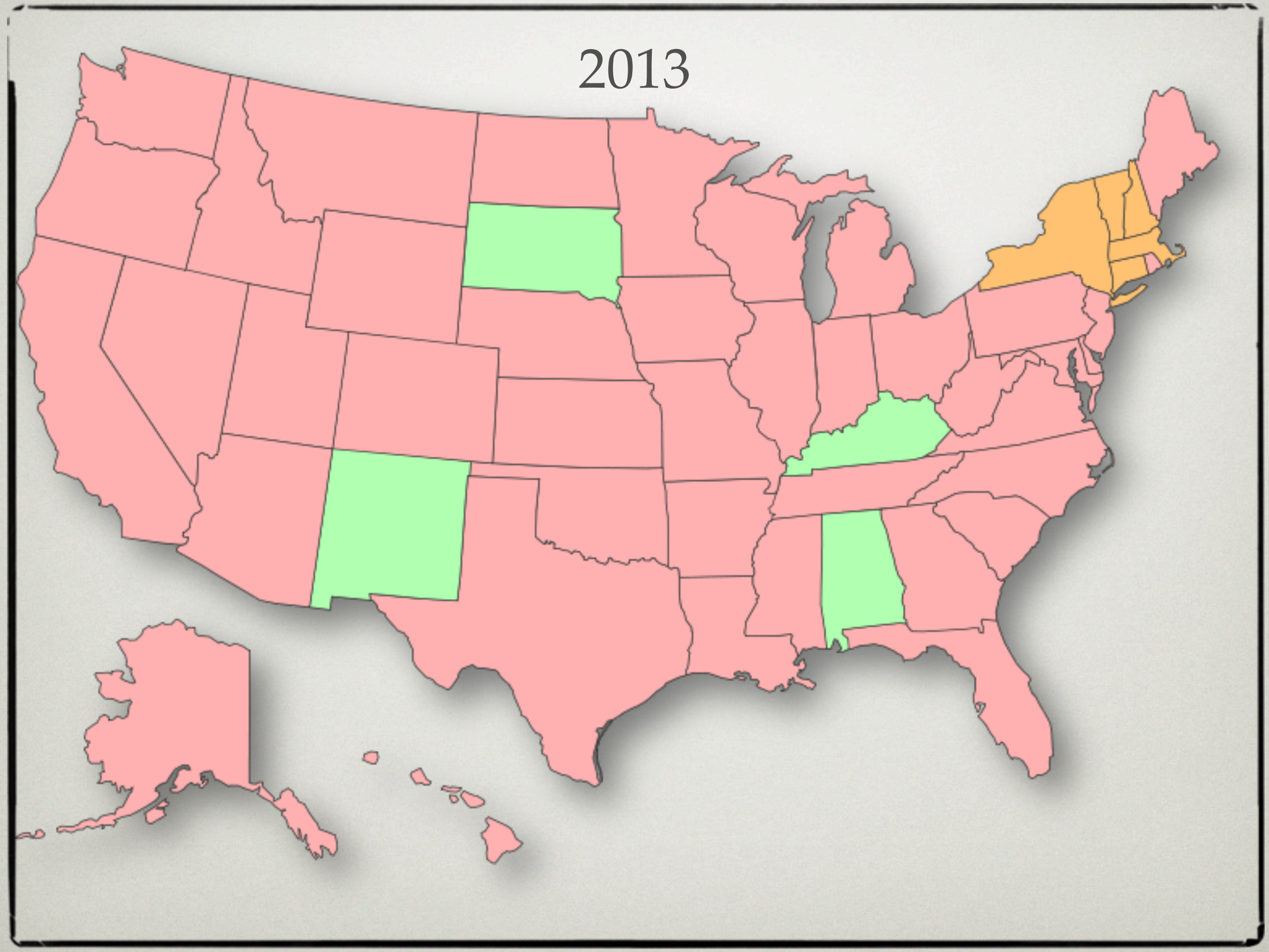
State

Breach-Notification Laws


2002


2003


2012


2013

2013


FEDERAL TRADE COMMISSION ★ UNITED STATES OF AMERICA ★ MCMXV ★

FTC v. Cbr Systems Inc.

FTC v. Cbr Systems Inc.

- 300,000 customer SSN's and credit card information exposed...

FTC v. Cbr Systems Inc.

- 300,000 customer SSN's and credit card information exposed...
- ... via unencrypted backups

FTC v. Cbr Systems Inc.

- 300,000 customer SSN's and credit card information exposed...
- ... via unencrypted backups
- FTC claimed that failure to encrypt the backups was "failure to use reasonable and appropriate procedures"

FTC v. Cbr Systems Inc.

- 300,000 customer SSN's and credit card information exposed...
- ... via unencrypted backups
- FTC claimed that failure to encrypt the backups was "failure to use reasonable and appropriate procedures"
- Privacy policy thus deceptive under FTC Act (15 U.S.C. § 44)

FTC v. Cbr Systems Inc.

FTC v. CBR Systems Inc.

- Company agreed to settle, but had to...

FTC v. Cbr Systems Inc.

- Company agreed to settle, but had to...
  - Establish, implement and maintain a "comprehensive security program"

FTC v. Cbr Systems Inc.

- Company agreed to settle, but had to...
  - Establish, implement and maintain a "comprehensive security program"
  - Designate accountable employees

FTC v. Cbr Systems Inc.

- Company agreed to settle, but had to...
  - Establish, implement and maintain a "comprehensive security program"
  - Designate accountable employees
  - Make biennial assessments and reports for 20 years by CISSP, CISA or GIAC professionals

FTC v. Franklin Toyota

FTC v. Franklin Toyota

- Because Franklin offered financial products (like loans and leases), the FTC alleged that the dealership was a financial institution under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(3)(A)

FTC v. Franklin Toyota

- Because Franklin offered financial products (like loans and leases), the FTC alleged that the dealership was a financial institution under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(3)(A)
- Frankin had a privacy policy, but still did not provide customers with annual privacy notice with clear opt-out ability

FTC v. Franklin Toyota

FTC v. Franklin Toyota

- P2P file-sharing software was installed on Franklin's computer network

FTC v. Franklin Toyota

- P2P file-sharing software was installed on Franklin's computer network
- Approximately 95,000 customer's SSN's and DLN's, addresses, DoB's available

FTC v. Franklin Toyota

- P2P file-sharing software was installed on Franklin's computer network
- Approximately 95,000 customer's SSN's and DLN's, addresses, DoB's available
- FTC contended that having P2P file-sharing on network was evidence of lack of "reasonable measures"

FTC v. Franklin Toyota

FTC v. Franklin Toyota

- Franklin entered into a consent agreement with the FTC

FTC v. Franklin Toyota

- Franklin entered into a consent agreement with the FTC
- New in-house measures required

FTC v. Franklin Toyota

- Franklin entered into a consent agreement with the FTC
- New in-house measures required
- Biennial audits by CISSP, CISA or similar professionals

FTC v. Franklin Toyota

- Franklin entered into a consent agreement with the FTC
- New in-house measures required
- Biennial audits by CISSP, CISA or similar professionals
- See also *FTC v. Wyndham Worldwide Corp.*, 2:12-cv-01365-SPL (D. Ariz. filed June 26, 2012) (Co. violated own policies)

Conclusions

Conclusions

- Cybersecurity can affect:

Conclusions

- Cybersecurity can affect:
  - Relations with vendors/contractors/customers

Conclusions

- Cybersecurity can affect:
  - Relations with vendors/contractors/customers
  - The character (and thus the cost and value) of the company infrastructure

Conclusions

- Cybersecurity can affect:
  - Relations with vendors/contractors/customers
  - The character (and thus the cost and value) of the company infrastructure
  - Investors

Conclusions

- Cybersecurity can affect:
  - Relations with vendors/contractors/customers
  - The character (and thus the cost and value) of the company infrastructure
  - Investors
  - Law Firms!

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act

- Passed in 1986

The Computer Fraud and Abuse Act

- Passed in 1986
- First directed to (rare) hacking

The Computer Fraud and Abuse Act

- Passed in 1986
- First directed to (rare) hacking
- Allows criminal *and* civil causes of action

The Computer Fraud and Abuse Act

- Passed in 1986
- First directed to (rare) hacking
- Allows criminal *and* civil causes of action
- Law expanded several times (1989, 1994, 1996, 2001, 2002, and 2008)

The Computer Fraud and Abuse Act

- Passed in 1986
- First directed to (rare) hacking
- Allows criminal *and* civil causes of action
- Law expanded several times (1989, 1994, 1996, 2001, 2002, and 2008)
- Another revision now before Congress

The Computer Fraud and Abuse Act

- Passed in 1986
- First directed to (rare) hacking
- Allows criminal *and* civil causes of action
- Law expanded several times (1989, 1994, 1996, 2001, 2002, and 2008)
- Another revision now before Congress
- Multiple controversies, most surrounding "authorization" and criminalization

Type 1 Activity

Type 1 Activity

- First modus of accessing information illegally -- by circumventing code-based restrictions

Type 1 Activity

- First modus of accessing information illegally -- by circumventing code-based restrictions
- Well established that this type of hacking is a potential felony under the CFAA

Type 1 Activity

- First modus of accessing information illegally -- by circumventing code-based restrictions
- Well established that this type of hacking is a potential felony under the CFAA
- See, e.g., *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)

Type 2 Activity

Type 2 Activity

- Second modus of accessing information illegally -- by violating a Terms of Service restriction

Type 2 Activity

- Second modus of accessing information illegally -- by violating a Terms of Service restriction
- Questionable but definitely possible in civil cases

Type 2 Activity

- Second modus of accessing information illegally -- by violating a Terms of Service restriction
- Questionable but definitely possible in civil cases
- Recently tried in criminal cases

Type 2 Activity

Type 2 Activity

- *United States v. Nozal*, 642 F.3d 781 (9th Cir. 2011) (No criminal prosecution for violating employer's Terms of Service)

Type 2 Activity

- *United States v. Nozal,* 642 F.3d 781 (9th Cir. 2011) (No criminal prosecution for violating employer's Terms of Service)
- Congress considering expressly allowing criminalization (or not) of Type 2 activities by amending the CFAA

Forfeiture and Seizure Cases

United States v. Arnold

United States v. Arnold

- 523 F.3d 941 (9th Cir. 2008)

United States v. Arnold

- 523 F.3d 941 (9th Cir. 2008)
- No Probable Cause needed

United States v. Arnold

- 523 F.3d 941 (9th Cir. 2008)
- No Probable Cause needed
- No Reasonable Suspicion needed

United States v. Arnold

- 523 F.3d 941 (9th Cir. 2008)
- No Probable Cause needed
- No Reasonable Suspicion needed
- @ border crossings

United State v. Cotterman

United State v. Cotterman

- 637 F.3d 1068 (9th Cir. 2011), reh'g granted, 673 F.3d 1206 (9th Cir. 2012), (9th Cir. *en banc*, No. 09-10139)

United State v. Cotterman

- 637 F.3d 1068 (9th Cir. 2011), reh'g granted, 673 F.3d 1206 (9th Cir. 2012), (9th Cir. *en banc*, No. 09-10139)

- Reasonable Suspicion Required

United State v. Cotterman

- 637 F.3d 1068 (9th Cir. 2011), reh'g granted, 673 F.3d 1206 (9th Cir. 2012), (9th Cir. *en banc*, No. 09-10139)
- Reasonable Suspicion Required
- Broadly interpreted

Questions?

Questions?

Ronald L. Chichester, Esq.

Ron@TexasComputerLaw.Com

http://www.TexasComputerLaw.com

713.302.1679