Morgan Lewis

DOING BUSINESS IN THE GOLDEN STATE

# PRIVACY AND CYBERSECURITY: THE TAIL THAT WAGS THE DOG

Reece Hirsch, Mark Krotoski, and Jenny Harrison

May 3, 2017

# Presenter: Reece Hirsch

- Partner in the Privacy and Cybersecurity and Healthcare practices

- Advises clients on development of privacy and security compliance programs, security breach response and planning, online privacy policies, mobile app privacy and the Internet of Things

- Special expertise in HIPAA and digital health privacy issues. Member of the editorial advisory boards of *Bloomberg BNA's Health Law Reporter*, *Healthcare Informatics* and *Briefings on HIPAA*

- Served on two advisory groups to the California Office of Privacy Protection (now part of the Department of Justice) that developed recommended practices for security breach response and medical identity theft prevention

**Phone: 415-442-1422;**
**Email: Reece.Hirsch@morganlewis.com**

# Presenter: Mark Krotoski

- Litigation partner in the Privacy and Cybersecurity and Antitrust practices.
- Advises clients on developing effective Cybersecurity and Trade Secret Protection Plans and in responding to a data breach incident or misappropriation of trade secrets. He has written extensively on these issues.
- Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the Department of Justice (DOJ) in Washington, D.C., and as a CHIP prosecutor in Silicon Valley, among other DOJ leadership positions.
- Successfully led prosecutions and investigations of nearly every type of international and domestic computer intrusion, cybercrime, and criminal intellectual property cases.
- Specialized on foreign economic espionage cases involving the theft of trade secrets with the intent to benefit a foreign government. He and his team successfully prosecuted two of the first foreign economic espionage cases authorized by DOJ under the Economic Espionage Act.

**Phone: 650-843-7212;**

**Email: Mark.Krotoski@morganlewis.com**

# Presenter: Jenny Harrison

- Litigation Associate focusing on cybersecurity and privacy matters.

- Advises clients on responding to a data breach incidents and maintaining proper and secure data collection and storage methods, as well as the development of privacy and security compliance programs.

- Has written extensively on cybersecurity issues, including foreign economic espionage, cybersecurity implications on SEC reporting, and current health care privacy matters.

**Phone: 415-442-1426;**
**Email: Jenny.Harrison@morganlewis.com**

# California -- The Cutting Edge of Privacy Regulation

- California continues to be a trend-setter in privacy and identity theft law.

- A *de facto* national standard.

- CA has often been a first-adopter of new types of laws that are later passed by other states, such as:
  - Security breach notification
  - Social Security number disclosure
  - General, reasonable security requirements

# California – The Cutting Edge of Privacy Regulation

- Other CA privacy laws remain unique on the national landscape:
  - "Shine the Light" direct marketing law
  - California Online Privacy Protection Act

- If you want to understand the future direction of privacy and security regulation, the California Legislature is a good place to start

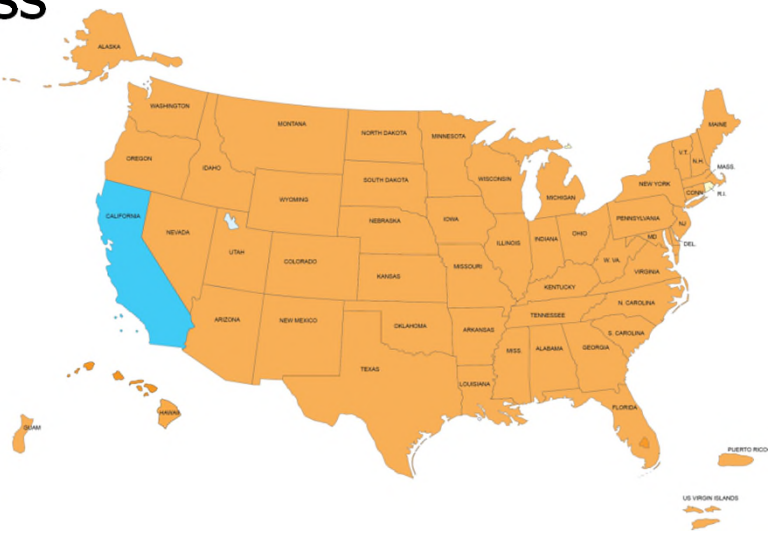
# Overview

- California's groundbreaking data breach notification law
- California Online Privacy Protection Act
- California Attorney General guidance on mobile app privacy
- Social Security number disclosure law
- The "Shine the Light" law governing direct marketing disclosures
- California reasonable security law
- Enforcement actions and issues
- Responding to a data breach
- The future of California privacy and cybersecurity regulation

# CALIFORNIA'S GROUNDBREAKING DATA BREACH NOTIFICATION LAW

# CA Data Breach Notification

- First Data Breach Notification Statute
  - Effective July 1, 2003
  - Enacted Sept. 25, 2002
    - Cal. Civ. Code § § 1798.29, 1798.82
- State agency, or a person or business conducting business in California
  - That owns or licenses computerized data that includes personal information
  - Notice to any California resident whose unencrypted personal information
  - Was, or is reasonably believed to have been, acquired by an unauthorized person
  - May bring a civil action to recover damages



# CA Data Breach Notification

Translate Website | Traducir Sitio Web

Search

State *of* California
Department *of* Justice

*Xavier Becerra ~ Attorney General*

Home | About the AG | In the News | Careers | Services & Information | Programs A-Z | Contact Us

Cybersafety › eCrime › Search Data Breaches

## SEARCH DATA SECURITY BREACHES

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (You can read the law here: California Civil Code s. 1798.29(a) for state agencies and California Civ. Code s. 1798.82(a) for businesses).

The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Below is a list of those sample breach notices. (Note that in some cases the organization that sent the notice is not the one that experienced the breach. For example, a bank may notify of a credit card number breach that occurred not at the bank, but at a merchant.)

You can search by the name of the organization that sent the notice, or simply scroll through the list. To read a notice, click on the name of the organization in the list. Then click on the link titled "Sample Notification."

Organization Name:

Date of Breach Range: From To

E.g., 2017-04-30 E.g., 2017-04-30

Search Clear

### Data Security Breach ( SB24 )

Data Security Breach Reporting
Submit Data Security Breach
Search Data Security Breaches

### Related Information

2016 Data Breach Report, pdf
Breach Help: Tips For Consumers
Cybersafety
Data Breach Statistics, pdf
eCrime
Identity Theft
Privacy

# State Laws

- 52 US Jurisdictions
  - 48 state data breach notification laws
    - New Mexico most recent state in April 2017
    - Excluding Alabama and South Dakota
  - Also DC, Guam, Puerto Rico and the U.S. Virgin Islands

# CA Data Breach Notification

- Preliminary Key Issues:
  - "Personal information" of a California resident?
    - Note expanding definition
  - Whether the information was encrypted?
  - Whether there was a "breach of the security" of the data?
    - Was the "personal information" was acquired, or was reasonably believed to have been acquired, by an unauthorized person?

# Expanding Definition of Personal Information


- "Personal information" means either of the following:

(1) An **individual's first name or first initial and last name** in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

# Expanding Definition of Personal Information


- "Personal information" means either of the following:

  (1) An **individual's first name or first initial and last name** in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

  (A) Social security number.

  (B) Driver's license number or California identification card number.

  (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

  (D) Medical information.

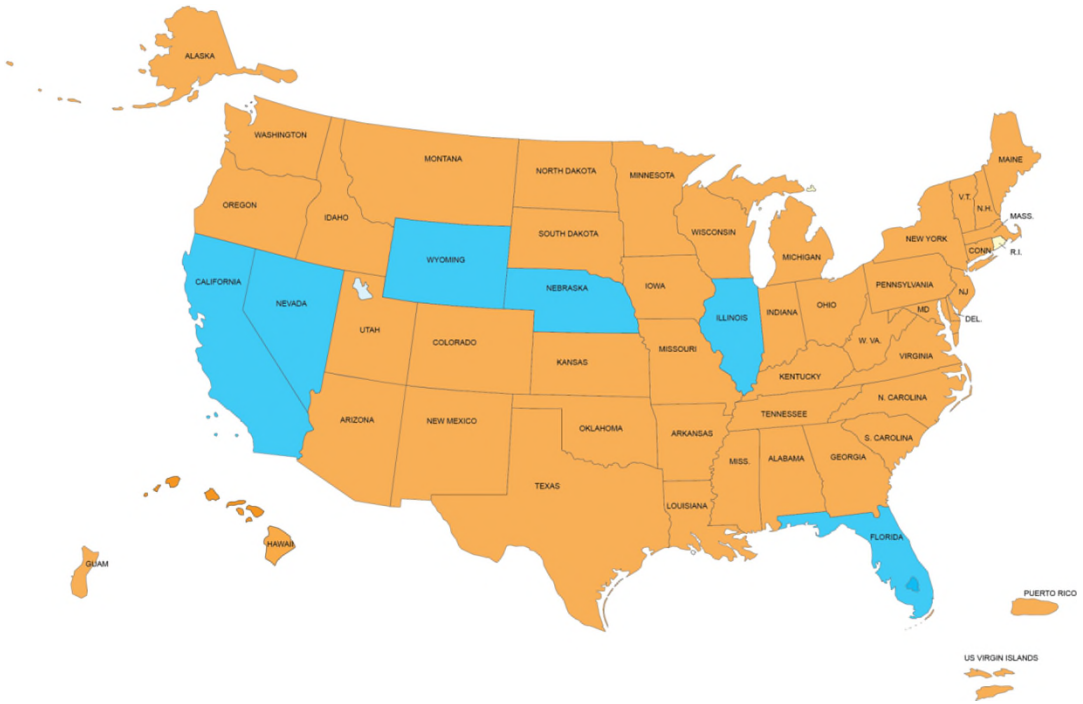
  (E) Health insurance information.

  (F) Information or data collected through the use or operation of an automated license plate recognition system.

  (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

# Expanding Definition

- Adding Usernames or Email Addresses
  - California (2014)
  - Florida (2014)
  - Wyoming (2015)
  - Nebraska (2016)
  - Nevada (2016)
  - Illinois (2017)



# Form of Notice

- Specific notice requirements
- California
  - Plain language, titled "Notice of Data Breach"
  - Use "the following headings:
    - "What Happened"
    - "What Information Was Involved"
    - "What We Are Doing"
    - "What You Can Do"
    - "For More Information"
  - Format "designed to call attention to the nature and significance of the information"
  - Title and headings "clearly and conspicuously displayed"
  - Text "no smaller than 10-point type"

[NAME OF INSTITUTION / LOGO] _____ _____ Date: [insert date]

NOTICE OF DATA BREACH

| | |
|---|---|
| What Happened? | |
| What Information Was Involved? | |
| What We Are Doing. | |
| What You Can Do. | |

Other Important Information.

[insert other important information]

| | |
|---|---|
| For More Information. | Call [telephone number] or go to [Internet Web site] |

Cal. Civ. Code § 1798.82(d)(1)

# Encryption Safe Harbor


- Disclosure of the breach:
  - (1) whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person, or,
  - (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the **encryption key or security credential** was, or is reasonably believed to have been, **acquired by an unauthorized person** and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

# CALIFORNIA ONLINE PRIVACY PROTECTION ACT

# Online Privacy Notice Law

- The California Online Privacy Protection Act of 2003 ("CalOPPA")
- Effective July 1, 2004
- Requires an operator of a commercial website or online service that gathers "personally identifiable information" (PII) to provide notice of privacy policy so that consumers are informed of potential disclosure, sale or sharing of information
- Law is unique to California but it impacts every national company with a website that collects PII of CA residents

# Online Privacy Notice Law

- The FTC's jurisdiction over privacy is largely based upon its authority under Section 5 of the FTC Act to regulate "unfair or deceptive acts or practices"
- Once a company posts a privacy policy, it may form the basis for a Section 5 action if its statements are deemed to be misleading, deceptive or inaccurate in describing privacy practices
- While it is a best practice to be transparent about privacy practices by posting a notice, CalOPPA is unique in imposing a general requirement to post a notice
  - Apart from industry-specific notice requirements under HIPAA, GLBA and state insurance privacy laws

# Online Privacy Notice Law

- "Personally identifiable information" is individually identifiable information collected:
  - Online
  - By an operator of a commercial website or online service
  - Maintained in accessible form

# Online Privacy Notice Law

- "Personally identifiable information" includes:
  - First and last name
  - Home or other address, including street name and name of city
  - E-mail address
  - Telephone number
  - Social Security number
  - Any identifier permitting physical or online contact
  - Any information concerning a user maintained in combination with one of these identifiers

# Online Privacy Notice Law

- Privacy policy must be conspicuously posted and:
  - Identify categories of PII collected and third parties with whom PII may be shared
  - Describe process for notifying consumers of material changes to policy
  - If operator maintains a process for individual to review and request changes to PII, describe that process
  - Identify the effective date of the policy

# Online Privacy Notice Law

- Effective January 1, 2015, CalOPPA was amended to give California minors a way to remove information they post online
  - Websites, online services, online apps or mobile apps must permit
  - A minor (anyone under 18) who is a registered user of the service or site
  - To remove, or request removal, of information posted by the minor
  - Notice of the minor "delete" option must be provided to minors, along with a statement that the "delete" option does not guarantee complete removal of the content

# Online Privacy Notice Law

- Often leads to a bifurcated minor privacy provision in online privacy notices
  - Federal Children's Online Privacy Protection Act (COPPA) imposes different requirements and applies to children under 13

- This CalOPPA amendment also prohibits:
  - Marketing or advertising certain products to minors, such as firearms, tobacco or dietary supplements
  - Knowingly using or disclosing the personal information of a minor for marketing or advertising purposes

# Online Privacy Notice Law

- Effective January 1, 2014, CalOPPA was amended to require that privacy policies must disclose whether the website or online service will honor "do not track" signals from Web browsers
- Does not require compliance with a do-not-track signal, merely a statement of whether signals are honored or not
  - The World Wide Web Consortium (W3C) has been slow to develop Do Not Track standards, but a proposal was finally released in 2015
- Also requires that notices include information about whether other parties may collect personal information about the California consumer's online activities over time and across websites when the consumer is using the operator's website or service ("cross-site tracking")

# Online Privacy Notice Law

- "Conspicuously posted" means:
  - Text of policy on homepage or first significant page after entering website
  - Icon link to policy on homepage or first significant page
    - Must include the word "privacy"
    - Color must contrast with background or be otherwise distinguishable
- Text link on homepage or first significant page:
  - Must include the word "privacy"
  - Must be in capital letters equal to or larger than surrounding text
  - Larger type than surrounding text or in contrasting type, font or color
- Other "reasonably accessible means" of making policy available

# Online Privacy Notice Law

- Good news – an operator is in violation of CalOPPA only if it fails to post a compliant policy within 30 days after being notified of noncompliance

- If companies fail to correct posted policies within 30 days they may face fines of up to $2,500 per violation
  - which may include each time a non-compliant app is downloaded

# Online Privacy Notice Law

- Takeaways:
  - If your privacy policy collects personal information of CA residents, does it:
    - Address processing of do-not-track signals?
    - Offer the minor "delete button" option?
    - Have an effective date?
    - Describe the process for reviewing and requesting changes to PII collected through the service (if you have one)?
  - If not, then your privacy policy should be updated to reflect CalOPPA
- For more useful guidance, see "Making Your Privacy Practices Public" from CA AG (May 2014)

# CALIFORNIA ATTORNEY GENERAL GUIDANCE ON MOBILE APP PRIVACY

# Mobile App Privacy

- The proliferation of mobile apps poses unique privacy concerns:
  - Collection of enormous volumes of personal information by smart phones and tablets
  - Ability to tie that data to specific individuals through geolocation data
  - Complex ecosystem of players (operating systems, app developers, ad networks)
  - Difficulty in providing robust privacy disclosures on small mobile device screens

# FTC Advice on Mobile Privacy

- February 2013:  FTC Staff Report "Mobile Privacy Disclosures: Building Trust Through Transparency"
  - Offers suggestions on privacy transparency for mobile platforms and app developers
  - Generally consistent with the California Attorney General's (AG's) January 2013 privacy recommendations for the mobile ecosystem
  - As in many other areas, California spurs the national privacy conversation

# California Mobile App Privacy Enforcement

- Early 2012: California AG announced a Joint Statement of Principles endorsed by companies whose platforms comprise the majority of the mobile app market
  - Focus on privacy transparency and compliance with CalOPPA

- October 2012: California AG issues warning letters to companies for failure to post mobile app privacy policies compliant with CalOPPA
  - AG views CalOPPA as applicable to mobile apps and other operators of online services that collect personal information of California residents

# Recommended Mobile App Privacy Practices

- January 2013:  CA AG issues "Privacy on the Go: Recommendations for the Mobile Ecosystem"
- AG's recommendations are consistent with subsequent FTC guidance
- Be Transparent
  - Make privacy policy available before the app is downloaded through the app store
  - Make privacy policy readily accessible within the app
  - Draw users' attention to data practices that may be unexpected or that involve sensitive information
    - "Just in time" notifications
    - "Surprise minimization"

# Recommended Mobile App Privacy Practices

- Limit Data Collection
  - Avoid collection of PII for uses not related to your app's basic functionality
  - Limit data retention to period necessary to support the intended function or meet legal requirements
  - Avoid or limit collection of sensitive information (financial, medical)
  - Use an app-specific or other non-persistent device identifier rather than a persistent, globally unique identifier
  - Give users control over the collection of PII used for purposes other than the app's basic functions
  - Default settings should be privacy protective

# CALIFORNIA SSN DISCLOSURE LAW

# Social Security Number Disclosure Law

- Cal. Civil Code Section 1798.85
- Limits use and disclosure of SSNs
- Affects any individual or nongovernmental entity doing business in California
- Intended to limit identity theft and restrain consumer reporting agencies that are accessing personal information through SSNs
- First-of-its-kind law that was copied by a number of other states
- CA AG issued a recommended practices document on protecting SSNs in April 2008

# SSN Disclosure Law

- Five prohibited uses of SSNs:
  - May not publicly post or display an SSN
  - May not print an SSN on any card required for access to products or services (insurance cards, employee badges)
  - May not require an individual to transmit SSN over Internet unless connection is secure or SSN is encrypted
  - May not require an individual to use SSN to access website, unless an additional password or other authentication device must also be used to access site.

# SSN Disclosure Law

- May not print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires SSN to be on document.
  - Exception: applications and forms sent by mail, including documents:
    - sent as part of an application or enrollment process
    - To establish, terminate or amend account
    - To confirm accuracy of SSN

- Statute does not prevent:
  - Collection, use or release of an SSN if required by state or federal law
  - Use of an SSN for internal verification or administrative purposes

# CALIFORNIA REASONABLE SECURITY LAW

# Reasonable Security Law

- Civil Code Section 1798.81.5, effective January 1, 2005
  - Also known as A.B. 1950
- First-of-its-kind "reasonable security" law

- Several other states, including Massachusetts and Nevada, have followed suit with much more prescriptive reasonable security laws, but CA was the first
- Has not been enforced thus far but 2016 statements by CA AG suggest that may change

# California Reasonable Security Law

- Basic mandate is fairly simple:
  - A business that owns or licenses personal information about a California resident shall
  - Implement and maintain reasonable security procedures and practices
  - Appropriate to the nature of the information
  - To protect the personal information from unauthorized access, destruction, use, modification or disclosure

# Reasonable Security Law

- "Personal information" means:
  - an individual's first name or first initial AND last name
  - IN COMBINATION WITH one of the following, when either the name or the other data elements are not encrypted or redacted:
    - Social Security number
    - Driver's license number or CA Identification Card number
    - Account number, credit card number , in combination with any required security code, access code or passcode that would permit access to a financial account.
    - Medical information.
- Does not include information that is publicly available through federal, state or local government records.

# Not Subject to Security Statute

- A provider of health care, health care service plan or contractor regulated by the Confidentiality of Medical Information Act
- A financial institution regulated under the Financial Code or SB 1
- A HIPAA covered entity
- An entity subject to confidentiality provisions of Vehicle Code regarding driver's license info
- A  business that is regulated by a state or federal law providing greater protection for personal information
- Reasonable security law a gap-filler – intended to cover businesses that are not regulated under industry-specific CA privacy laws

# Relationship to Security Breach Notification Law

- Complements CA's security breach notification law
- Definitions of "personal information" are similar
- Breach notification law created an incentive for businesses to adopt reasonable security practices – A.B. 1950 imposes an affirmative legal obligation to do so

# Contracting Requirement

- A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party
- Must require by contract that the party implement and maintain reasonable security procedures and practices
  - Appropriate to nature of the information
  - To protect the information from unauthorized use or disclosure
- Only applies when disclosures are pursuant to a contract
- Does not require that parties enter into a contract when they didn't previously
- No sample contract language has  been issued

# The Big Question

- What are reasonable security procedures and practices?
- No specific guidance on security practices – lets businesses exercise their own judgment as to what level of security is appropriate UNTIL
- February 2016: CA AG in its California Breach Report stated that "failure to implement all the [Center for Internet Security's Critical Security] Controls that apply to an organization's environment constitutes a lack of reasonable security" under CA's security law
- The 20 controls in CIS Critical Security Controls represent a comprehensive security program
- How will the AG apply and enforce this standard in the future?

# THE "SHINE THE LIGHT" LAW GOVERNING DIRECT MARKETING DISCLOSURES

# "Shine the Light" Law (Marketing Disclosures)

- Marketing Disclosure ("Shine the Light") Law (Civil C. §1798.83-.84)
- Applies to all businesses with 20 or more full or part-time employees
  - That have established a business relationship with a customer residing in California
  - And have, within the immediately preceding year, disclosed the customer's information
  - To third parties
  - For direct marketing use
- Businesses that engage in these direct marketing disclosures must, upon request, disclose the type of personal information shared and the names and addresses of the recipient entities

# "Shine the Light" Law (Marketing Disclosures)

- "Direct marketing purposes" does not include use of personal information to effectuate a customer's transaction
- Financial institutions subject to S.B. 1 are exempted from Shine the Light
- As an alternative to providing a Shine the Light notice, a business may comply with the law by implementing a privacy policy allowing customers to opt-in or opt-out of direct marketing information sharing
- Sometimes privacy policies state that company complies with Shine the Light as applicable – a potentially misleading approach

# "Shine the Light" Law (Marketing Disclosures)

- There has been a spate of class action lawsuits in recent years based on Shine the Light
- In February 2014, the Ninth Circuit affirmed dismissal of three Shine the Light class actions
  - In each case the plaintiffs failed to prove that they had been injured by the companies' alleged lack of disclosures under the law
  - Other cases have been dismissed because the plaintiffs' failure to make a disclosure request
- Companies that are subject to Shine the Light must have proper procedures in place to respond to requests and must be able to respond within required timeframes

# Industry-Specific Privacy Laws

- Confidentiality of Medical Information Act (Civil C. § 56 *et seq.*)
- Insurance Information and Privacy Protection Act (Ins. C. § 791 *et seq.*)
- Financial Information Privacy Act (Fin. C. § 4050 *et seq.*) (S.B. 1)
  - One of the more stringent state financial privacy laws
  - Generally expands upon the floor set by Gramm-Leach-Bliley Act
  - Example: S.B. 1 requires opt-in for sharing nonpublic personal information with a nonaffiliated third party
    - GLBA requires opt-out

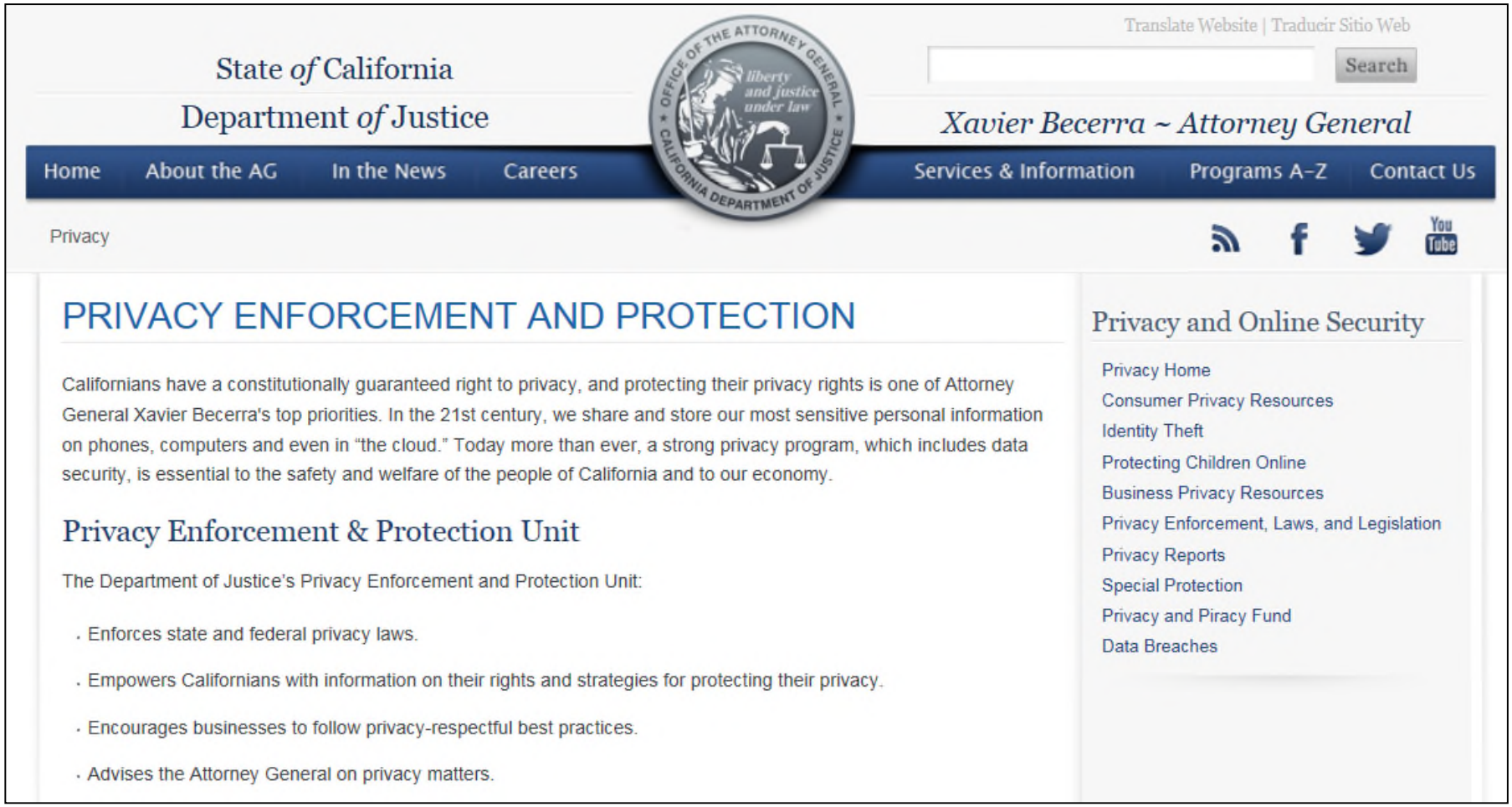
# California Constitution

- *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.*

  -Article 1, Section 1 of the California Constitution

# ENFORCEMENT ACTIONS AND ISSUES

# California Privacy Enforcement & Protection Unit



Translate Website | Traducir Sitio Web

Search

State *of* California
Department *of* Justice

*Xavier Becerra ~ Attorney General*

Home | About the AG | In the News | Careers | Services & Information | Programs A–Z | Contact Us

Privacy

## PRIVACY ENFORCEMENT AND PROTECTION

Californians have a constitutionally guaranteed right to privacy, and protecting their privacy rights is one of Attorney General Xavier Becerra's top priorities. In the 21st century, we share and store our most sensitive personal information on phones, computers and even in "the cloud." Today more than ever, a strong privacy program, which includes data security, is essential to the safety and welfare of the people of California and to our economy.

### Privacy Enforcement & Protection Unit

The Department of Justice's Privacy Enforcement and Protection Unit:

- Enforces state and federal privacy laws.
- Empowers Californians with information on their rights and strategies for protecting their privacy.
- Encourages businesses to follow privacy-respectful best practices.
- Advises the Attorney General on privacy matters.

### Privacy and Online Security

- Privacy Home
- Consumer Privacy Resources
- Identity Theft
- Protecting Children Online
- Business Privacy Resources
- Privacy Enforcement, Laws, and Legislation
- Privacy Reports
- Special Protection
- Privacy and Piracy Fund
- Data Breaches

# Increasing Enforcement and Regulatory Scrutiny

- Civil Enforcement
  - FTC
  - FCC
  - SEC
  - State Attorneys General
  - State Financial Service Regulators
  - Plus, CFTC / NFA

- Law Enforcement
  - DOJ
  - FBI
  - USSS
  - DHS

# Civil Enforcement Issues

- Fines

- Cease and desist
- Censure
- Injunctive action

- Establishing a comprehensive security program
  - Address security risks
  - Protect data
- Initial and biennial cybersecurity or data assessments
- Term of agency jurisdiction

# RESPONDING TO A DATA BREACH

# Overseeing Internal Investigation

- Initial call
- Determine scope and nature of breach
  - Roller coaster of ups and downs
- Attorney client privilege
  - Is the privilege effectively in place?
- Assess legal consequences
  - What regulatory agencies?
  - Was information accessed, acquired, or exfiltrated?
  - Which customers?
  - What legal standards apply?

# Role of Attorney Client Privilege

- For the purpose of seeking or providing legal advice
  - Aids in the careful evaluation of any threats/intrusions and responsive action for investigation, legal obligations, and litigation
  - Early in the process
  - Risks if not properly used/protected
- Company counsel working with outside counsel
- Role of counsel with vendors
  - At the direction of counsel

# Initial Investigative Questions

- Scope of the breach
  - When did the compromise occur?
    - Early assessments can be revised
  - When and how was breach discovered?
- How breach occurred?
- Who caused breach?
  - Attribution analysis
- What cyber risks?
- Remediation steps

# State Laws

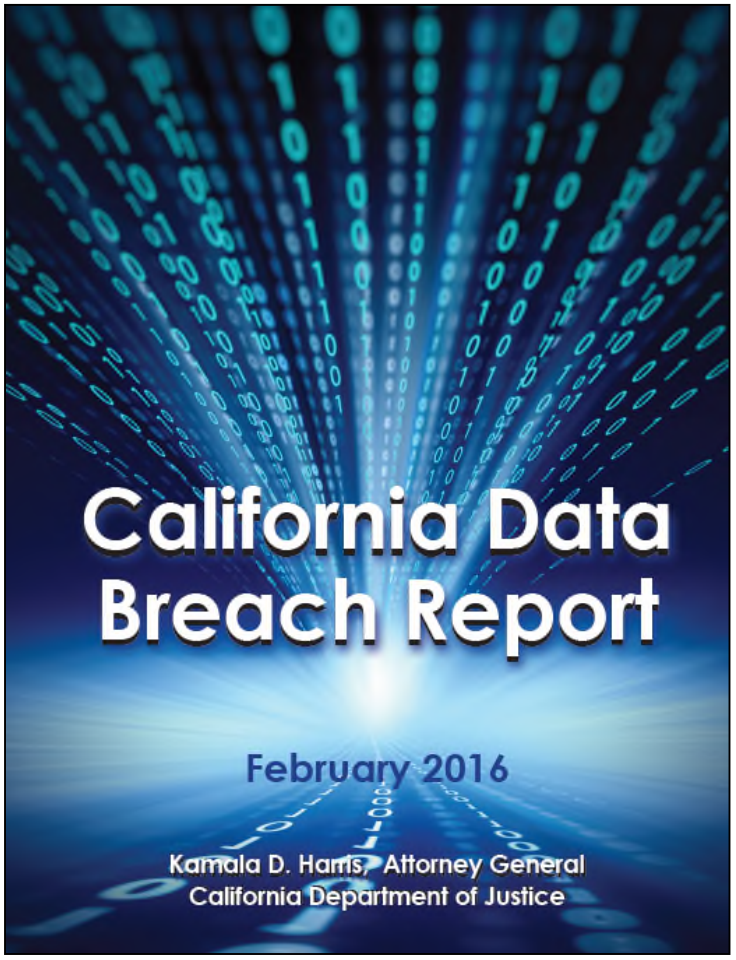
- 52 US Jurisdictions
  - 48 state data breach notification laws
    - New Mexico most recent state in April 2017
    - Excluding Alabama and South Dakota
  - Also DC, Guam, Puerto Rico and the U.S. Virgin Islands

# Differing State Notification Standards

- Who must be notified?
  - Customers
  - Government
- When must they be notified?
  - Reasonable notice
  - Delayed notification
- What data (PII) triggers notification?
- What constitutes a "data breach"?
  - What exemptions?
  - Any reasonable likelihood of harm?
- What form of notice is required?
  - Email notification
  - Substitute notice
- What consequences and penalties?
  - Private right of action
- Any there any industry-specific requirements?
  - Insurance (GA, KS, ME, MT)
  - Medical records (CA, LA)
  - Financial institutions (MN)
  - Public utilities (MI)

# Differing State Notification Standards

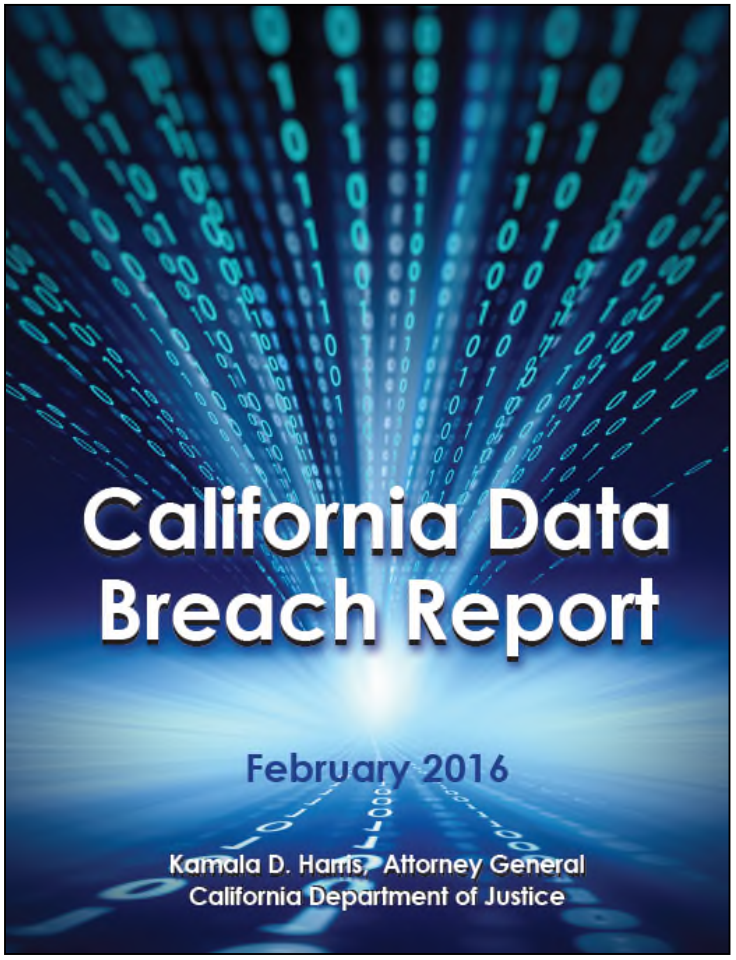
- "There is a range of definitions of personal information.
  - All state laws include the basic types in the original California law (Social Security number, driver's license number, financial account number).
  - Eight states (17 percent), including California, add **medical information**, and five (11 percent), including California, add **online account credentials**.
  - Thirteen states (28 percent), including California, add other types of information, with **health insurance information**, **biometric information**, and **taxpayer ID** being the most common."




https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf?

# Differing State Notification Standards

- "19 states (40 percent), including California, have **specific content requirements for notices**.
  - A few have additional, unique content requirements. For example, the Massachusetts 23law prohibits disclosing the nature of the breach or the number of residents affected in the notice, and the Wisconsin law requires the notice to tell the recipient to make a written request to learn the personal information involved.
- Twenty-five states (53 percent) require a breached organization to **notify the state Attorney General and/or another government agency**."






https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf?

# THE FUTURE OF CALIFORNIA PRIVACY AND CYBERSECURITY REGULATION

# What's Next In Privacy Legislation and Regulation?

- February 2017:  Sen. Hannah-Beth Jackson (D-Calif) introduced S.B. 327
- Would impose requirements on manufacturers to equip Internet of Things devices with "reasonable security features appropriate to the nature of the device and the information it may collect, contain or transmit"
- Response to September 2016 DDOS attack on major sites using IoT devices

# What's Next In Privacy Legislation and Regulation?

- For a glimpse into the future of state and federal privacy and identity theft legislation and regulation, keep an eye on California
- California AG's office has been a de facto national regulator under Kamala Harris?
  - Will that trend continue under new AG Xavier Becerra?
- Will states have greater say if Trump Administration causes federal agencies to step back privacy regulation?

# Questions


**Reece Hirsch**
San Francisco, California
tel. +1.415.442.1422
fax. +1.415.442.1001
reece.hirsch@morganlewis.com



**Mark Krotoski**
Silicon Valley, California
tel. +1.650.843.7212
fax. +1.650. 843.4001
mark.krotoski@morganlewis.com



**Jenny Harrison**
San Francisco, California
tel. +1.415.442.1426
fax. +1.415.442.1001
jenny.harrison@morganlewis.com

# THANK YOU

**ASIA**

Almaty
Astana
Beijing
Singapore
Tokyo

**EUROPE**

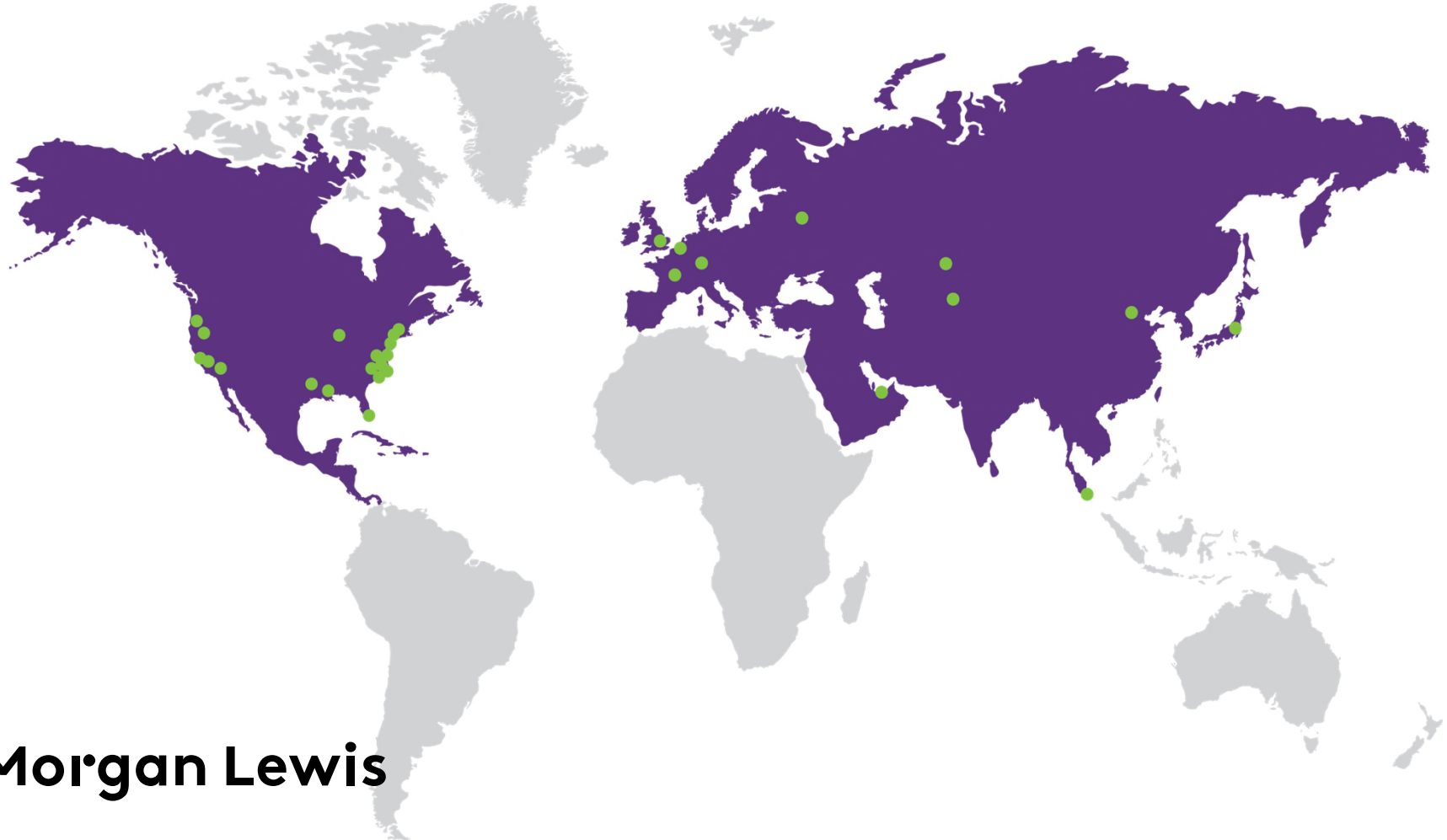
Brussels
Frankfurt
London
Moscow
Paris

**MIDDLE EAST**

Dubai

**NORTH AMERICA**

Boston
Chicago
Dallas
Harrisburg
Hartford
Houston
Los Angeles
Miami
New York
Orange County
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Washington, DC
Wilmington



Morgan Lewis