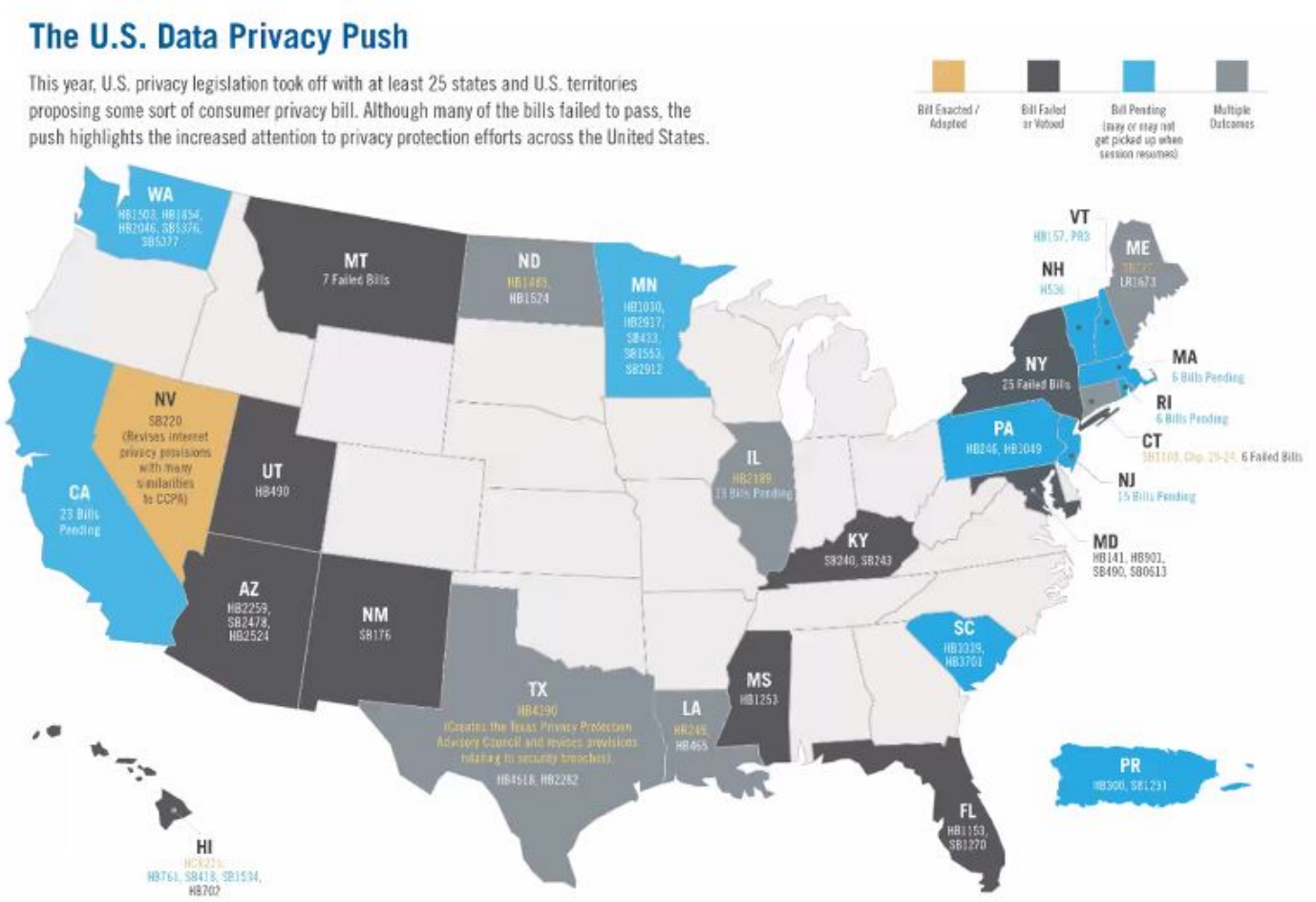
Privacy & Data Security Regulation: Implications for RIM & IG

Boise Valley ARMA

October 22, 2020

State data privacy laws



State data privacy laws

- Focus on the (current) “big three”
  - California’s Consumer Protection Act (CCPA)
  - New York’s Stop Hacks and Improve Electronic Data Security (SHIELD) Act
  - Illinois’ Biometric Information Privacy Act (BIPA)
- Even sharper focus on the Records and Information Management (RIM) and Information Governance (IG) requirements (express and implied)

Today's speakers

John Isaza

David Shonka

Martin Tully

Ken Withers

PRIVACY & DATA SECURITY REGULATION:

IMPLICATIONS FOR RIM & IG

Access®

John Isaza, Esq.

john.isaza@rimonlaw.com

John.Isaza@AccessCorp.com

949-632-3860

John is a California-based attorney, VP Information Governance Solutions at Access Corp featuring Virgo™, a cloud-based software for records management and global research, and partner at Rimon, where he chairs the privacy and information governance practice.

Mr. Isaza is one of the world's foremost experts in the field. He has developed privacy, information governance and records retention programs for some of the most highly regulated Global 1000 companies.

Why was CCPA Significant?

- First comprehensive, “GDPR-like” privacy law in U.S.
- California is the 5th largest economy in the world (~40 Million people)
- Ramifications for organizations across the U.S. and beyond
- Adds fines and both private and public rights to sue
- Opens the door for follow-on legislation from other states & federal gov’t
- Anticipate the pace of data privacy and data protection/security regulation to accelerate!

Access

Key Consumer Rights Granted by CCPA

With respect to personal information (PI) relating to that consumer (held by a business):

- The right to request a business to delete any personal information about the consumer collected by the business – with certain exceptions
- Disclosure: A business that collects PI about a consumer is required to disclose the consumer's right to delete their PI on its web site or in its online privacy policy or policies.
- Limited right to bring legal actions for damages & fines

Issues with the Right to Request/Delete

- Verifiable consumer request – How do we verify? No regulations as yet, but verifying someone making a request is who they say the are is problematic
- Where do you begin looking?
- How do you know you've got it all?
- Conducting a thorough search may be problematic and/or costly

Another Sticking Point: “Sale” of Information

- **“Sale” means:** Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by a business to another business or third party for monetary or valuable consideration.
- **Exceptions:**
  - Consumer uses or directs business to intentionally disclose personal information to a third party, as long as the third party does not subsequently sell the PI
  - Consumer uses business to “intentionally interact” with a third party
  - Business uses or shares PI that is “necessary to perform a business purpose”
  - PI is transferred as part of a merger, acquisition, bankruptcy, or other transaction in which third party assumes control of the business

Key Changes to the California Privacy Rights Act (CPRA) Ballot Measure

Special rules regarding "Sensitive Personal Information" which includes SSNs

Right to limit the use of Sensitive personal information collected

Changes to definitions, including "publicly available information."

Changes to the exemptions section, adding an exemption for information submitted by job applicants

Establishment of a California Privacy Protection Agency for enforcement and court-like administrative procedures for violations

Why it Matters to You

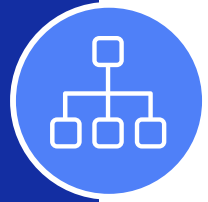
It's a requirement!

In all data protection and privacy programs implementing strong security safeguards to protect personal data is paramount.

- Reduce security incidents
- Reduce privacy breaches

The standards are increasingly written into law

The standards are increasingly explicitly called out in contract terms



Either explicitly or by implication, standards and contractual terms applicable to you are also applicable to business partners with whom you share data

And Your Business Partners

GDPR standard contractual clauses

Obligate you and every business partner with whom you share data to comply with GDPR privacy and security requirements

- You are liable for issues and violations of partners

Once you become obligated, you have **no choice** to also obligate your business partners

insert the standard clauses,
and/or ensure GDPR compliance

caveat: Privacy Shield Framework is now invalid

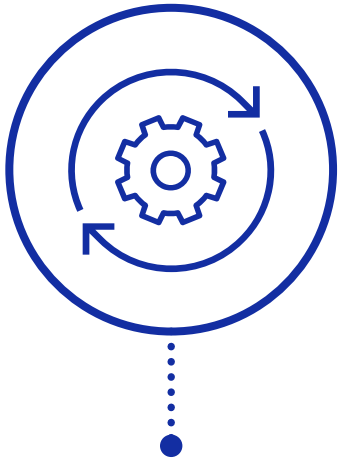
The Result

An interlocking series of contracts and obligations

Everybody is liable for everybody else

Joint and several liability

What Can You Do About All of This?



Stay compliant
know what the regulations (in each location) require

Be sure your data sharing partners are **compliant**

Know what your **contracts say**

- If you're on the receiving end of all that privacy and security boilerplate, read it
- Make sure you include all that boilerplate in the contracts with your own data sharing partners

Access

BIOMETRICS: What Does It Mean When You Are The Record?

Why Privacy Laws Don't Countenance Biometrics:

> "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. **Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse**, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."
>
> -- 740 ILCS 14/5(c) (emphasis added)

Illinois Biometric Information Privacy Act

- Enacted in 2008, but only took off later, in 2015
- Covers “biometric identifiers” and “biometric information”
  - **Biometrics identifiers** exclude:
    - Writing samples, written signatures, photographs, tattoo descriptions, height, weight, hair color, or eye color
    - Certain medical information, such as PHI under HIPAA
  - **Biometric information** means “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.”
- Applies to any private entity in possession of biometric identifiers or information; Excludes state or local government agencies.

Illinois Biometric Information Privacy Act

- Requires a written policy be made available to the public regarding retention and destruction of BI
- Requires prior written notice and consent to collection and purpose and term for which BI is collected, used, and stored
- Prohibits sale, lease, or trading of BI for profit
- Prohibits disclosure or redisclosure of BI without prior written notice and consent or required by law
- Mandates use of reasonable data security measures for storing and transmitting BI

Illinois Biometric Information Privacy Act

- Provides for a private right of action
- A prevailing party may recover for each violation:
  - For negligent violations - liquidated damages of $1,000 or actual damages, whichever is greater;
  - For intentional or reckless violations - liquidated damages of $5,000 or actual damages, whichever is greater;
  - Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
  - Any other relief, including an injunction, as the court may deem appropriate

Illinois BIPA Litigation: No Harm? No Problem!

- *Rosenbach v. Six Flags Entertainment Corp.* (Jan. 2019)
  - IL Sup. Ct. held that persons need not show actual or concrete harm in order to have a standing to sue under BIPA
  - Mere violation of the Act is enough
- Countless lawsuits already spawned
  - Over 200 BIPA lawsuits reportedly filed in 2018-2019 alone
  - Growing list of major companies have found themselves the subjects of BIPA violations, joining The Home Depot, Dr. Pepper, Walgreens, and WeWork
- Divergence of federal court decisions on injury
  - Facebook paid $550 million in a BIPA lawsuit settlement
  - Google won summary judgment based on finding of no concrete injury

Illinois BIPA Litigation: Inconsistent Results

- *Patel v. Facebook, Inc.* (9th Circuit, 2019)
  - Expanded ability to pursue BIPA claims for mere technical statutory violations by holding any BIPA violation amounts to a violation of plaintiffs' substantive privacy rights; thus, concrete injury-in-fact for Article III standing
  - Upheld certification of a class of Illinois Facebook users, finding Facebook's extraterritoriality and "runaway damages" arguments insufficient
- *Rivera v. Google* (N.D. Illinois, 2018)
  - Dismissed on summary judgement a BIPA lawsuit against Google pertaining to the company's photo app technology based on an absence of any concrete injury
- *Santana v. Take-Two Interactive* (2nd Circuit, 2017)
  - Held that NBA 2K players lacked standing to pursue BIPA claims because they suffered no actual injury or harm by the video game's collection and retention of their face scans

Illinois BIPA Litigation – A Runaway Train?

- Constitutional challenges to BIPA?
  - *Richard Rogers v. BNSF Railway Co.*, No. 19-cv-3083 (N.D. Ill. Oct. 31, 2019)
  - Rejected argument that BIPA conflicts with and is preempted by the Federal Railroad Safety Act, the Interstate Commerce Commission Termination Act, and the Federal Aviation Administration Authorization Act.
  - Judge Kennelly found BNSF's preemption argument "highly speculative, to say the least" because BNSF was unable to identify any federal regulation that governs the collection or storage of biometric information.
- Illinois Senate proposed a bill in March 2019 (SB 2134) which would eliminate the private cause of action

More BIPAs On The Horizon?

- Post-*Rosenbach,* biometric privacy bills were introduced in AZ, CT, FL, NH, NM, NY, OR and WA

Recordkeeping Considerations

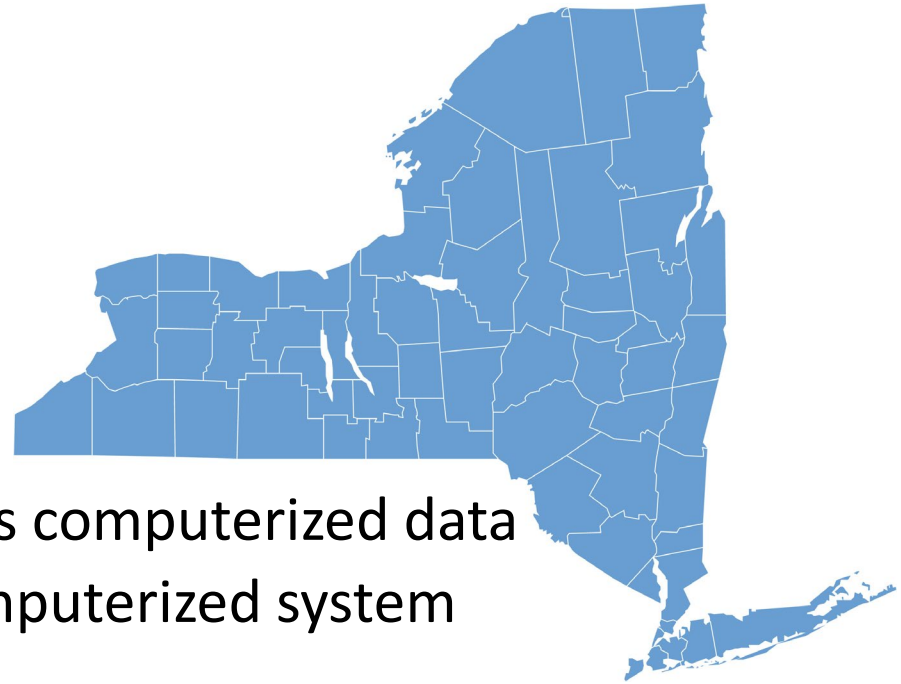
- A company may not collect biometric information without prior written consent
- Must develop and make available to the public a written retention policy for the eventual destruction of such data
- Also restricts the disclosure and dissemination of biometric information and regulates its storage

Some Biometric Takeaways

- Consider whether use of biometric technology is necessary and appropriate, especially if your organization has a presence in Illinois
- If relying on biometric technology, provide advance notice to the individuals and obtain consent
- Ensure that the notice adequately discloses what you collect, why you collect, how you use, how you store, and how and to who you disclose biometric data
- Include notice of biometric policies in “terms and conditions” and in the privacy policy
- Obtain written informed consent from each individual, when appropriate. Obtain new consent if purpose, usage, or sharing changes
- Unless disclosure is required by law, sharing biometric information with a third party is prohibited without individual’s prior consent, including with vendors and service providers
- Allow individuals to opt out of biometric information collection and sharing
- Stay informed of the latest legal developments in this area and work with outside counsel on implementing and updating relevant policies and procedures

New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)

- Provisions
  - Consumer Notifications
  - Mandated Security Requirements
  - Attorney General Enforcement
  - Covers
    - Any person or business that owns or licenses computerized data
    - Any person or business that maintains a computerized system
    - State entities



SHIELD Act
Key Terms

Personal Information

- Name, number, personal mark, or other identifier used to identify a natural person

Private Information *means either*

- Unencrypted personal information in combination with
  - Social Security Number
  - Driver's License Number or other identification card number
  - Account number with access codes for a financial account or
  - Account number without access code if that is sufficient to give access to a financial account
  - Biometric information
- Email address in combination with password or security answer giving access to online account

Small Business

- Less than 50 employees
- Less than $3 million in annual revenue in previous three years or
- Less than $5 million in year-end total assets

SHIELD Act
Principal Notice Provisions

- Mandatory expedient notice to any New York resident whose private computerized information is lost due to a breach of a security system or reasonably believed to have been accessed or acquired without valid authorization unless:
  - The loss is not likely to cause harm
  - Notice is given under another legal regimen (GLB, HIPPA, NY Code or Regs)
- Notice of determination to the state attorney general within 10 days if loss affects over 500 New York residents
- Notice to State AG of notice to consumers and to other regulators
- Notice to Credit Reporting Agencies

SHIELD Act
Form and Content of Notices

- Notice Form
  - Written
  - Electronic (consumer consent and log requirement)
  - Telephonic (log requirement)
  - Alternative substitutes in limited circumstances
    - Email (where addresses are available)
    - Conspicuous online posting
    - State media
- Notice Content
  - Contact information for the business
  - Contact information for state and federal agencies
  - Description of categories of lost information

SHIELD Act
Principal Security Provisions

- Owner or licensee of computerized information of New York residents
  - Designate one or more employees
  - Identify reasonably foreseeable internal and external risks
  - Assess sufficiency of safeguards
  - Train and manage employees
  - Selects and contracts with capable service providers
  - Adjust security requirements as needed
  - Maintains reasonable safeguards
    - Assesses network and software risks
    - Assesses processing, transmission, and storage risks
    - Detects, prevent and responds to attacks or system failures
    - Regularly tests and monitors effectiveness of key controls
  - Maintains physical safeguards
    - Assesses risks of storage and disposal
    - Detects, prevents, and responds to intrusions
    - Protects against unauthorized access of use, before during and after collection, transportation, and destruction or disposal
  - Prompt and Safe Disposal
- Small Business
  - Must maintain reasonable administrative, technical and physical safeguards appropriate to the size and complexity of its business, the nature and scope if its activities, and sensitivity of the information it maintains

SHIELD Act
Records for Notifications

Explicit

- Logs of Notification phone calls
- Logs of Computerized contacts

Implicit

- Consumer Notices
- State Notices
- Notification determinations
- Assessments of losses (or non-losses)
- Compliance with other regulations (GLB, HIPPA, State cods and regs)

SHIELD Act
Records for Security

Basic	Maintaining Reasonable Safeguards	Maintaining Physical Safeguards
• Security Plan and Procedures including Response Plan • Designation of responsible employee(s) • Internal/external risk assessments • Identification of threats and vulnerabilities • Remediation of threats and vulnerabilities • Employee and contractor training • Vendor contracts and audits • Remediation records	• Assessment of network and software risks • Records of network and software updates and patching • Assessments of processing, transmission, and storage risks • System logs • Monitoring logs and records	• Assessment of hardware and paper security • Processes for storage and disposal • Logs and records of access and intrusions • Off-site and mobile devices • Disposition records

Questions?
Comments?