DIGITAL TRANSFORMATION (DT)

Navigating the Patchwork of Cybersecurity and Data Privacy Laws

SEPTEMBER 21, 2021

Jeffrey Schultz, F. Scott Galt, Romaine C. Marshall, Partners at Armstrong Teasdale

Daniel Nelson, Digital Silence
Co-Founder/COO

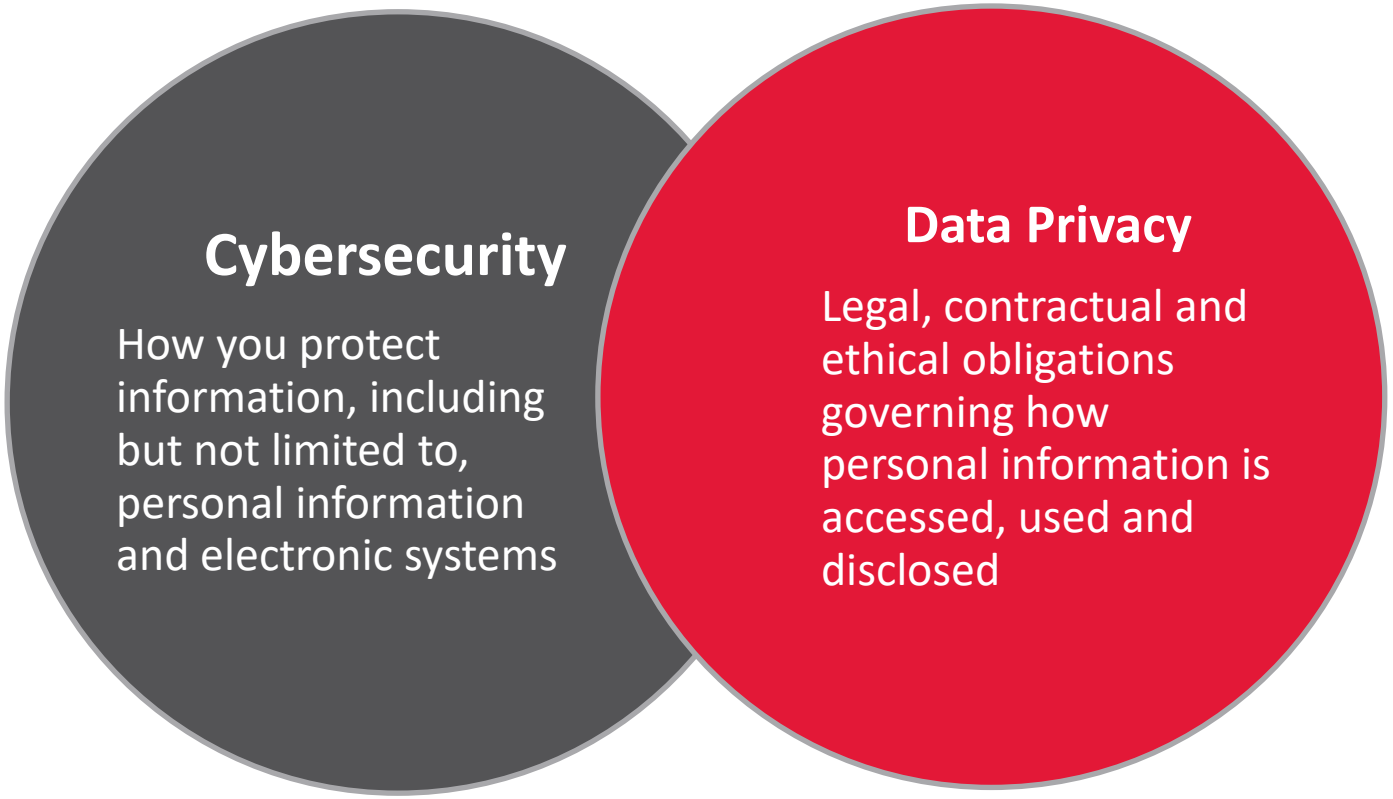
Always exceed expectations through teamwork and excellent client service.

AT Digital Transformation (DT) Fall Series

- ***Navigating the Patchwork of Cybersecurity and Data Privacy Laws that Govern***
  - Tuesday, Sept. 21, 2021
- ***Supply Chain Risk Management: a Cybersecurity and Data Privacy Imperative***
  - Tuesday, Oct. 26, 2021
- ***The Internet of Things, Emerging Technologies, and the Cybersecurity and Data Privacy Laws Implicated***
  - Wednesday, Dec. 8, 2021

https://www.armstrongteasdale.com/events/navigating-the-patchwork-of-cybersecurity-and-data-privacy-laws/

AT DT *Legal* Lens



Governed by a patchwork of legal, industry and regulatory standards

DT and the Pandemic

- ***The process of leveraging technology, people and processes to innovate and stay competitive***
- **During the pandemic, DT has resulted in increased interconnectivity leading to increased cybersecurity and data privacy risks**

Forbes Magazine, September 15, 2020, COVID-19 Is Transforming The Legal Industry: Macro and Micro Evidence.

A Blooming Cybersecurity Patchwork

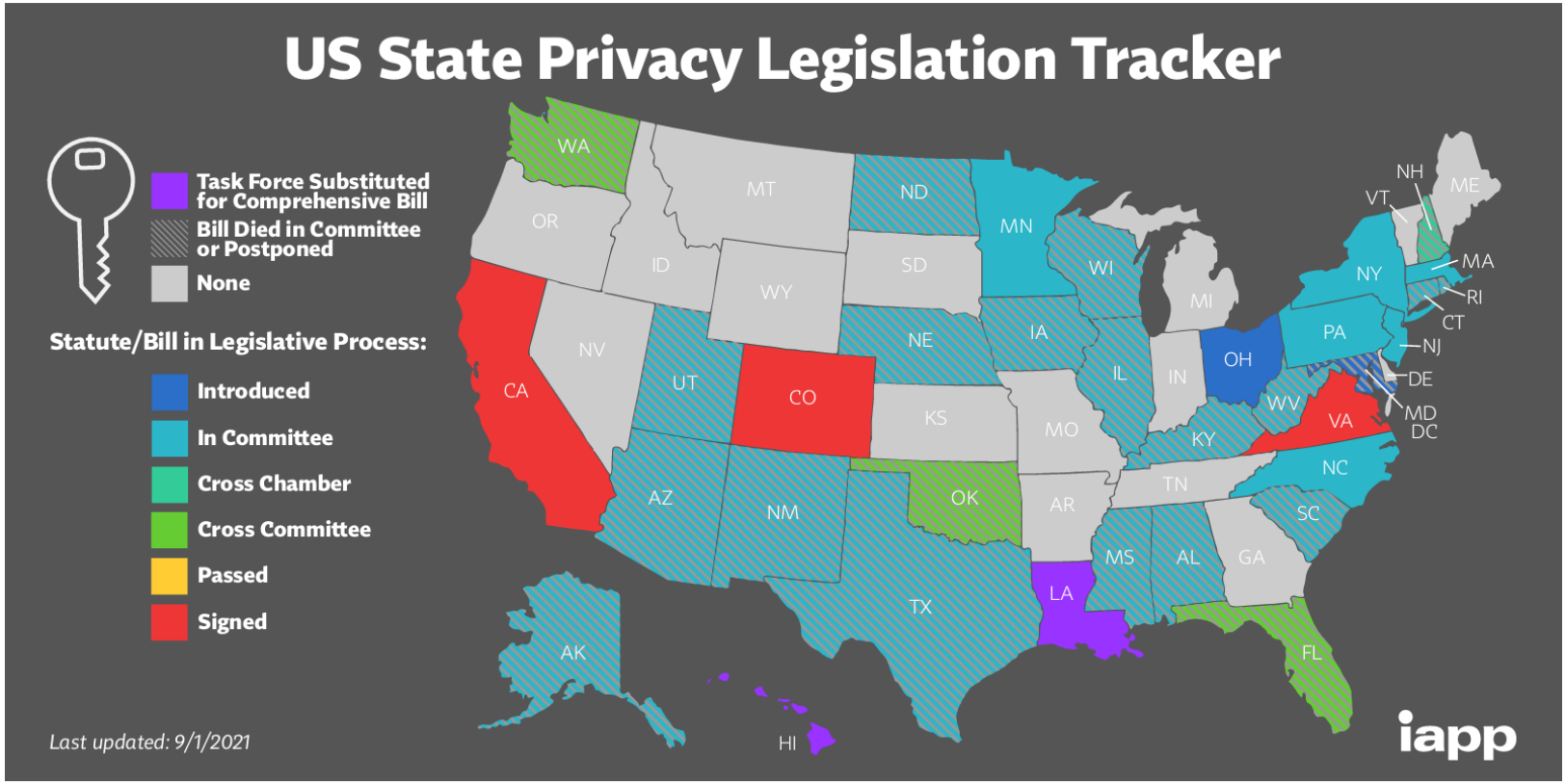
- **"At least 38 states, Washington, D.C., and Puerto Rico introduced or considered more than 280 bills or resolutions that deal significantly with cybersecurity."**
- **At least 20 states enacted 46 key cybersecurity-related bills in 2020**
- **E.g., Utah in the last five years:**
  - Utah Computer Abuse and Data Recovery Act (2016)
  - Utah Electronic Information or Data Privacy Act (2019)
  - Utah Cybersecurity Affirmative Defense Act (2021)
- **Data breach notification statutes now exist in every state**

Source: https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx.

Cybersecurity's Legal Landscape

- **Federal Trade Commission: "*What are the Industry Standards? Are We Meeting Them?*" in 2019 to "cybersecurity is not an IT issue but a board issue" in 2020.**
  - Now: lawmakers are asking for $1 billion in funding for the FTC to create a cybersecurity enforcement division.
- **Securities and Exchange Commission: New SEC boss wants to "stay abreast of [technological] developments" and "be ready to bring cases involving issues such as crypto, cyber, and fintech."**
  - Now: Five cybersecurity enforcement actions in the last two months – only one published before these, in 2018.

A Blooming Data Privacy Patchwork



Source: https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/

Data Privacy's Legal Landscape

- **General Data Protection Regulation:** *"The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it."*
  - Now: Amazon's
- **California Consumer Protection Act:** *"We will look kindly, given that we are an agency with limited resources, and we will look kindly on those that ... demonstrate an effort to comply."*
  - Now: new AG (Bonta) = new guidance, and new law (CPRA)
- **Oh and … last week the SEC announced a $10 million settlement against an app developer in a data privacy action.**

“Common Threads” Emerge

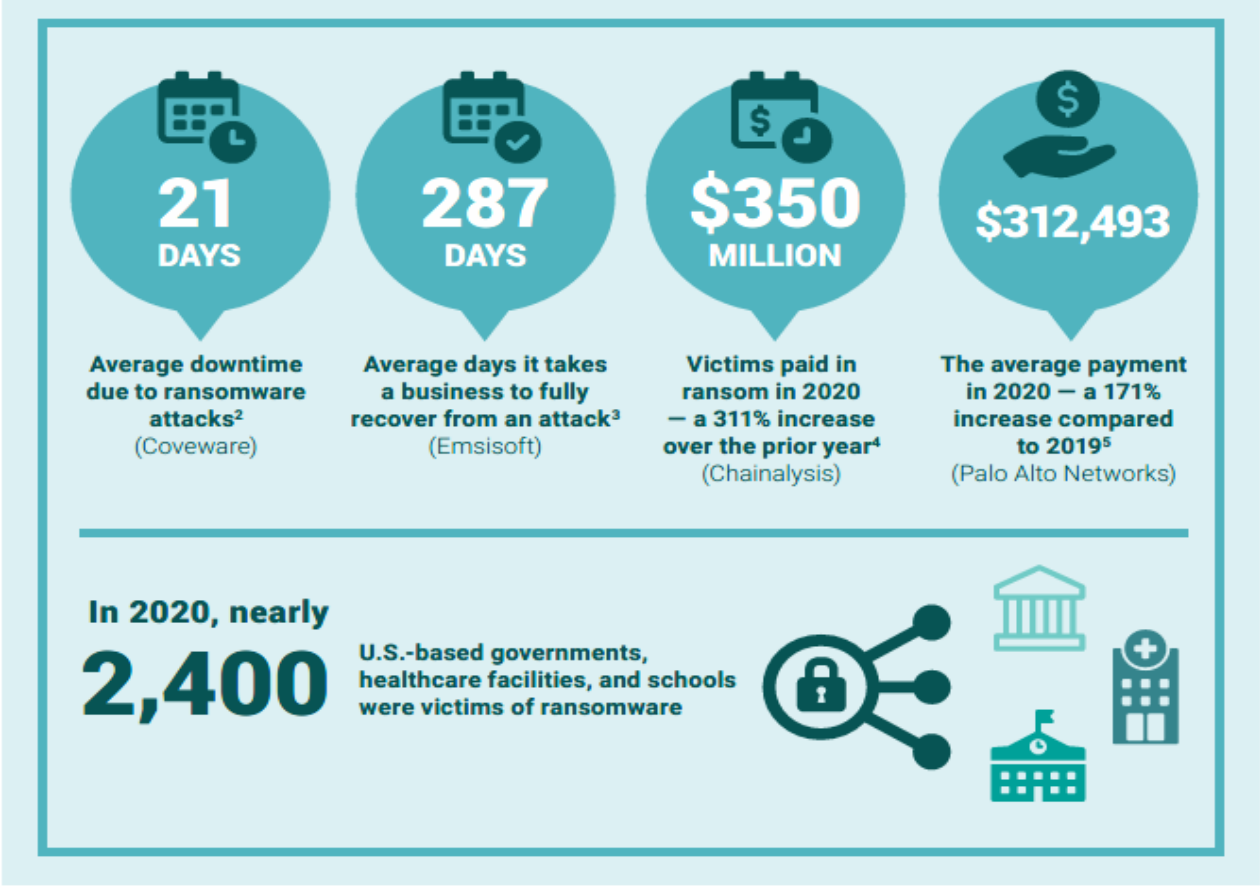
- **Thousands of incidents and hours helping clients have revealed certain PROTECTIONS and RESPONSES**
- **Cybersecurity**
  - Incident Response Plans (IRPs)
  - Risk Assessments (RAs)
  - Written Information Security Programs (WISPs)
- **Data Privacy**
  - Privacy Policies and Procedures
  - Privacy Reviews, Data Privacy Impact Assessments (DPIAs)

The Threats

DT as a Threat "Process"

- ***Blackbaud***
  - Incident: ransomware
  - Legal: multiple class actions and investigations
  - DT: quick acquisitions of other software platforms
- ***Morgan Stanley***
  - Incident: data breaches
  - Legal: class action
  - DT: closed data centers for "faster" software options
- ***Dunkin'***
  - Incident: data breaches
  - Legal: NY AG investigation, $650,000 fine
  - DT: deep dive into data and digital strategies

Ransomware



Combating Ransomware, A Comprehensive Framework for Action, by the Institute for Security + Technology, April 29, 2021 https://securityandtechnology.org/ransomwaretaskforce/report/

Laws and Regulations

(and Industry Standards)

Cybersecurity Liability Theories

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EUGENE BOLTON, on behalf of himself and all others similarly situated,

Plaintiff,

v.

ACCELLION, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Eugene Bolton ("Plaintiff") brings this Class Action Complaint on behalf of himself and all others similarly situated, against Defendant, Accellion, Inc. ("Accellion" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Businesses whose systems and products are designed and marketed for the purposes of storing and transferring sensitive, personally identifying information ("PII") and personal medical information[1] ("PMI") owe a duty of reasonable care to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PMI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals.

Bolton vs. Accellion

- **Accellion's alleged *duty* breaches included:**
  a) mismanaging its software and failing to identify reasonably foreseeable internal and external risks;
  b) allowing clients to continue utilizing the outdated FTA software for sensitive file transfers after Accellion knew it could not be maintained;
  c) failing to design and implement information safeguards;
  d) failing to adequately test and monitor the safeguards;
  e) failing to adjust its information security program; and
  f) failing to detect the breach at the time it began or within a reasonable time.

Bolton vs. Accellion

- **Alleged damages included:**
  a) theft and exposure of their PII and/or PMI;
  b) costs associated with requested credit freezes;
  c) the detection, prevention of ID theft and account use;
  d) purchasing credit monitoring and identity theft protection;
  e) unauthorized charges and loss of use of and access to funds;
  f) lowered credit scores;
  g) costs associated with time spent and the loss of productivity;
  h) damages to and diminution in value of their PII; and
  i) continued risk of exposure to hackers and thieves of their PII.

Data Privacy Laws and Regulations

- **EU/UK are already enforcing:**
  - €20 million or up to 4% of preceding year global turnover.
    - Amazon (Luxembourg DPA issues €746 million fine)
      WhatsApp (Ireland DPA issues €225 million fine)
  - U.K. fines and differences in enforcement / U.K. GDPR and EU GDPR are virtually identical
    - British Airways (£20 million), Marriott Hotels (£18.4 million)
    - Tend to work with companies after initial announcement

Data Privacy Laws and Regulations

- **In the U.S., we are entering the age of enforcement.**
  - CCPA: Enforcement letters re use of the opt-out tool. CA's AG Rob Bonta is serious. Plus private right of action.
  - Virginia's CDPA (no private right of action and 30-day cure period) .
  - Colorado's Privacy Act (no private right of action and 60-day cure period) .

Protections

You Should Implement

FBI Guidance

- Conduct regular training – inform employees of the IRP and practice the implementation of the IRP, at least annually.
- Back up data regularly – verify the integrity of those backups and test restoration procedures to ensure its working
- Secure your back ups – ensure that backups are not connected permanently to the computers and networks they are backing up.
- Devise an Incident Response Plan (IRP)

Combating Ransomware, A Comprehensive Framework for Action, by the Institute for Security + Technology, April 29, 2021
https://securityandtechnology.org/ransomwaretaskforce/report/

Incident Response Plan (IRP)

- **Why?**
  - A patchwork of laws: PCI, HIPAA, GLBA.
  - FTC: a reasonable plan, reasonably followed, may be the difference for a regulatory action.
  - SEC: recent enforcement actions have analyzed IRPs.
  - Insurance: an IRP is becoming mandatory by underwriters.
  - Reputational harm: consumers and other third parties increasingly intolerant of a botched response.
  - Business continuity: responding as important to survival than defending.

Incident Response Plan

- **What Should an IRP include?**
  - An Incident Response Team (IRT):
    - Individuals with *clearly defined roles and responsibilities*
  - Roles that:
    - provide timely, organized, and effective response;
    - avoid loss of or damage to IT systems, network, data;
    - minimize economic, reputational, or other harms; and
    - manage litigation, enforcement and other risks.

Main IRP elements

- **Phase 1 – Accountability**
  - Identifying the IRT, the IRT coordinator and duties
- **Phase 2 – Response Procedures**
  - Developing IR procedures
  - Severity classification
- **Phase 3 – Reporting and Notification**
  - Identifying obligations
- **Phase 4 – Post-incident Response**
  - IRP training, testing and review

Other IRP elements

- **Timing (and context) is *everything***
  - Ransomware
    - Insurance
    - Technical consultants
    - OFAC advisory
    - Internal investigations
- **Appendices and checklists matter**
  - Rosters, IRT contact info, notifications
  - Manageable customization

What Regulators Request

- **Interrogatory:**
  - Describe your risk assessment process, including but not limited to how the nature and level of risk is assessed and recorded, the frequency of risk assessment, and how the Company responds to . . . identified risks.

Why RA?

- **Risk assessments**
  - Lead to policies, then standards, then procedures, all of which together serve to comprehensively outline objectives and administrative, technical and physical controls.
- **Risk assessments should**
  - Should assess at least once every twelve months, internal and external risks to the security, confidentiality, or integrity of personal or sensitive information and systems.

Data Privacy Protections

- **Common Threads**
  - There is quite a lot at stake.
    - Understand imminent legislation and bring expertise in-house or develop from within.
  - Communication is king.
    - Top-down approach demonstrating that management takes seriously the cybersecurity/data privacy needs of the organization. And that your partners also understand your org's needs.
  - Know and own your data.
    - Know where it is (inflows and outflows) and own responsibility for it (data map/data processing register).

Responses

You Should Have Ready

Written Information Security Programs

- **Cybersecurity 'Safe Harbor' Laws**
  - Ohio, New York, Utah
  - Affirmative defenses to cybersecurity lawsuits stemming from data breaches
  - "Industry-recognized frameworks" required
- **Industry Standard Laws**
  - Oregon, Massachusetts, Rhode Island require WISPs
  - Must include administrative, technical and physical safeguards for personal information

Key WISP Elements

- **Examples of Administrative**
  - Proper training for employees about appropriate cybersecurity best practices
  - Auditing programs and practices regularly to ensure they are reasonable and appropriate considering the data collected and resources of the organization
  - Designating an employee to oversee the WISP
  - Maintaining an IRP

Key WISP Elements

- **Examples of Technical Controls**
  - Information Protection and Control
  - Vulnerability Assessments
  - Penetration Testing and Quarterly Scanning
  - Identity & Access Management
  - Detective Measures
  - Security Patches
  - Asset Management
  - Mobile Device Management
  - Email Management
  - Vendor Management

A WISP is a *Living* Document

FTC requires organizations to:

"Evaluate and adjust the [Written] Information Security Program in light of any changes to [your] operations or business arrangements …."

Safe Harbor Laws

Similarly, require that WISPs be adjusted "in light of changes or circumstances needed to protect the security, confidentiality, and integrity of personal information."

Data Privacy Responses

- **Common Threads**
  - Regulators take cooperation into account.
    - Be responsive and make good faith efforts now to have a compliance program in place.
  - Clarity is essential.
    - Make your privacy policy transparent and compliance tools user-friendly and be open to the need for privacy reviews/gap assessments.
  - Both legislation and the technology to help address it will continue to evolve.
    - Be poised to improve/update privacy policies and compliance procedures.

About Armstrong Teasdale

Armstrong Teasdale – Firm Information

For 120 years, Armstrong Teasdale has forged long-term relationships with clients large and small around the globe.

340+ LAWYERS

300+ STAFF

SERVING OVER **125+** FORTUNE 500 COMPANIES

AMLAW **200**

With 13 offices across the U.S. and in London, our lawyers are licensed to practice in 30 states plus Washington, D.C., as well as in the U.K., Germany and Ireland.

Jeffrey Schultz, Armstrong Teasdale

jschultz@atllp.com / 314.259.4732

Scott Galt, Armstrong Teasdale

sgalt@atllp.com / 314.259.4709

Romaine Marshall, Armstrong Teasdale

rmarshall@atllp.com / 801.401.1604

Daniel Nelson, Digital Silence Co-Founder /COO

Nelson@digitalsilence.com / 314.791.2514