

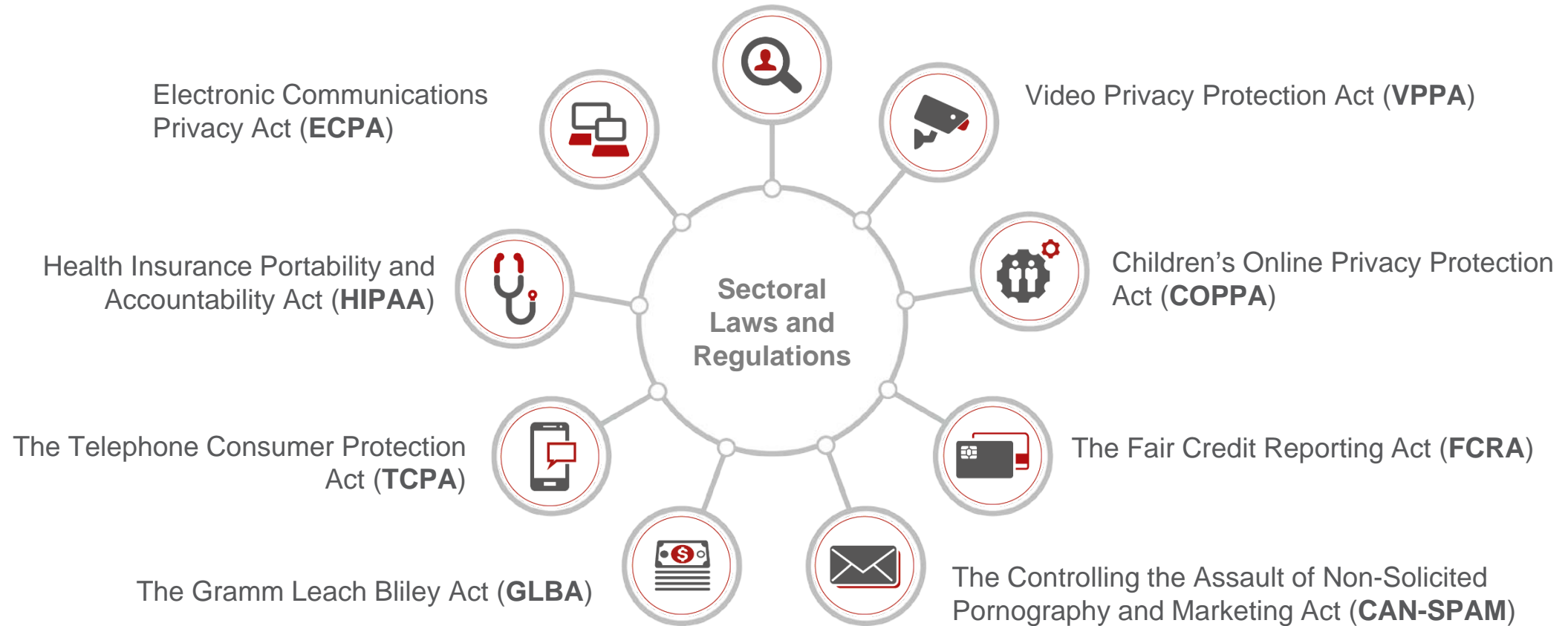


LATHAM & WATKINS

The Current US Data Privacy Regime

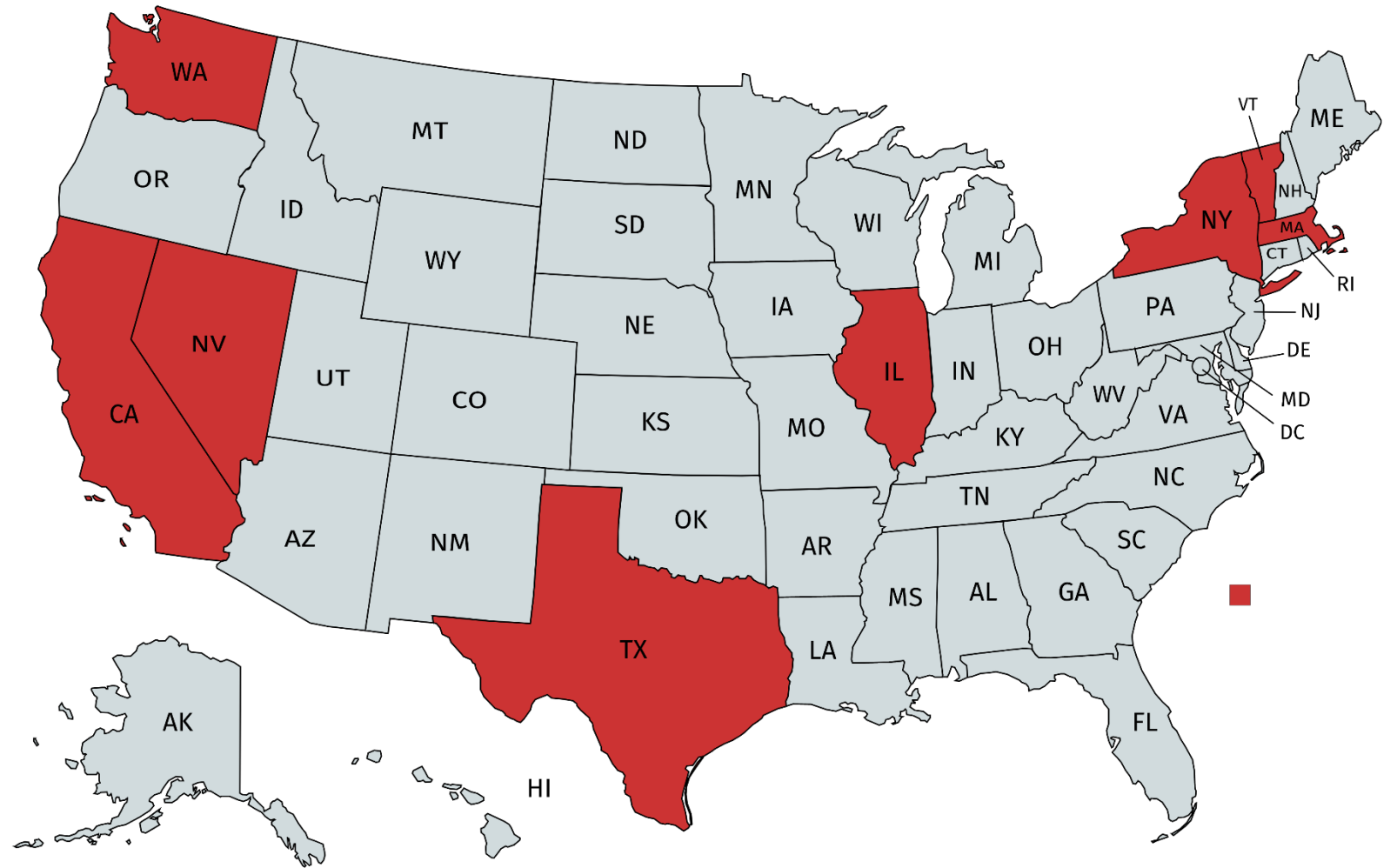
The Federal Patchwork

Section 5(a), Federal Trade Commission Act (**FTC Act**) (unfair or deceptive data protection practices)



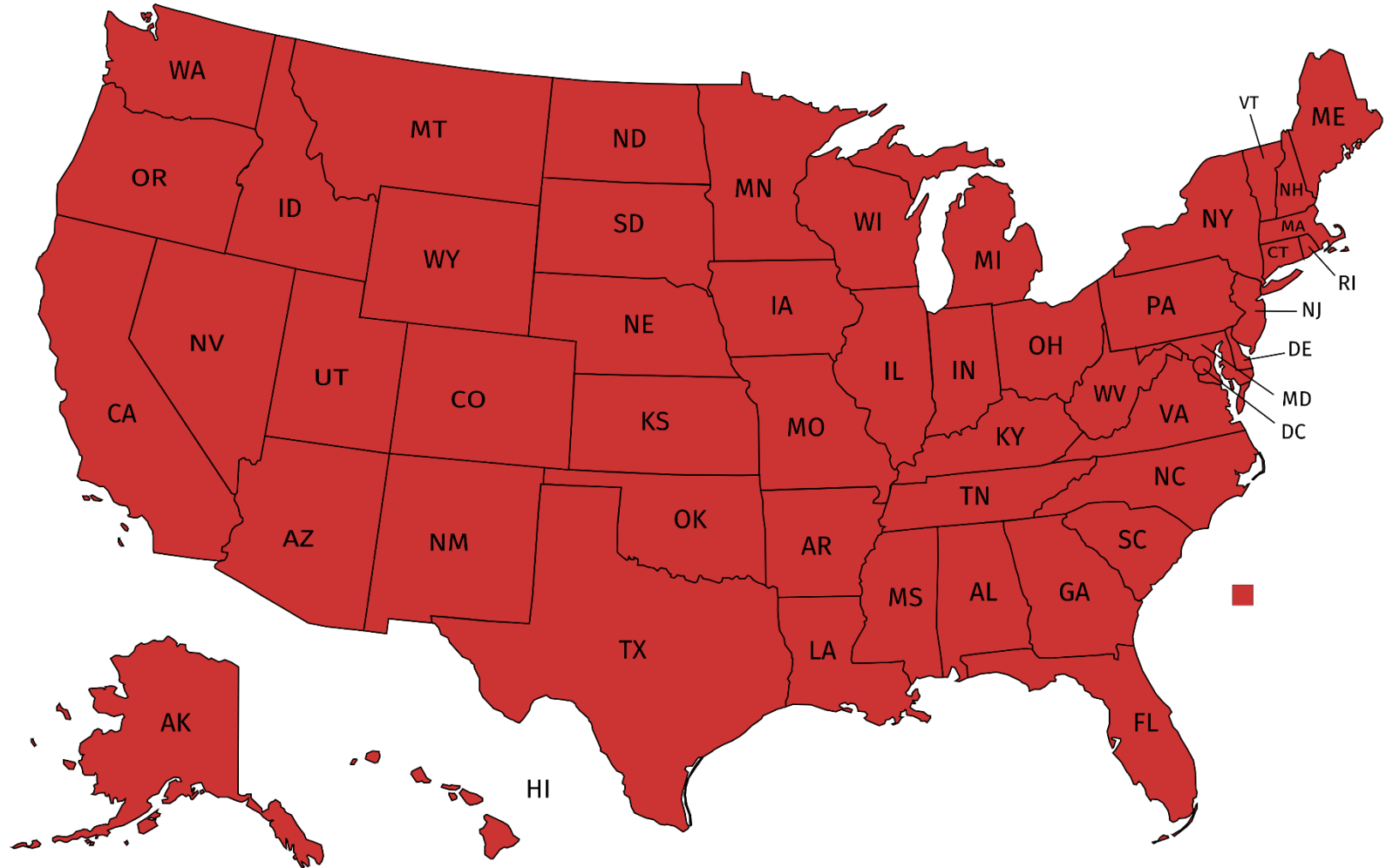
The State Laboratory

- Comprehensive regime **(CA)**
- Sale opt-out **(NV)**
- Biometrics **(IL, TX, WA)**
- Financial Regulator **(NY)**
- Mandatory security program **(MA, etc.)**



Data Breach Notification Requirements

- Varying, specific and inconsistent requirements – whether, when and how to notify
- Aggressive AG enforcement
- Consumer / AG notifications
- Some public state breach databases



Federal Trade Commission

- **Section 5(a)** of the FTC Act: "unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful" (15 U.S.C. Sec. 45(a)(1))
 - **Deceptive** practices occur when a statement or omission is likely to mislead a reasonable consumer and impacts a consumer's decision to buy or use a product.
 - **Unfair** practices are defined as those that "cause or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"
- Civil Investigative Demands, Access Letters, Informal Inquiries
- Administrative enforcement
- Civil Lawsuits
- Privacy and security cases available at <http://business.ftc.gov/legal-resources>

State Attorneys General



“Little FTC Act” and many Federal laws



Multi-state investigations



Easy path to civil monetary penalties,
but more flexible injunctive outcomes

- *Similar authority to FTC and many other Federal authorities*
- *Often act in parallel*

- *Often band together to leverage resources*
- *Lead by small committee of lead states*

- *State laws more liberally authorize civil penalties*
- *Consent Orders not always mandatory—Assurances Of Voluntary Compliance can be options*

Private Lawsuits



Privacy & Data Breach Class Actions

- *Consumer class actions*
- *Typically invoke a variety of federal and state laws*



Shareholder Derivative Lawsuits

- *Directors and officers could potentially be held liable for inadequately protecting a company's information.*



Lawsuits by other affected stakeholders

- *Banks, financial institutions, other clients affected by privacy and data breaches have brought claims*

Contact Information



Gail E. Crawford

Partner, London
Technology Transactions Group

T +44.20.7710.3001
M +44.7976.355.723
E gail.crawford@lw.com



Michael H. Rubin

Partner, San Francisco
Litigation & Trial

T +1.415.395.8154
M +1.415.425.7500
E michael.rubin@lw.com



Jennifer C. Archie

Partner, Washington, D.C.
White Collar Defense & Investigations

T +1.202.637.2205
M +1.571.217.5875
E jennifer.archie@lw.com



Robert Blamires

Counsel, San Francisco
Technology Transactions

T +1.415.395.8142
M +1.650.815.1061
E rober.blamires@lw.com

Disclaimer

Although this presentation may provide information concerning potential legal issues, it is not a substitute for legal advice from qualified counsel. Any opinions or conclusions provided in this presentation shall not be ascribed to Latham & Watkins or any clients of the firm.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.

© Copyright 2019 Latham & Watkins.