大成 DENTONS

CLE FOR IN-HOUSE COUNSEL
ST. LOUIS | JUNE 2019

Cyber Ethics: In-House Counsel's Ethical Role In Data Privacy and Cybersecurity

Peter Stockburger
Dentons
+1 619 595 8018
peter.stockburger@dentons.com

Agenda

- Overview of Regulatory and Legal Landscape
- Overview of ABA Model Rules on Privacy / Cybersecurity
- Key Takeaways
- Questions

Cyber Ethics

Overview of regulatory and legal landscape

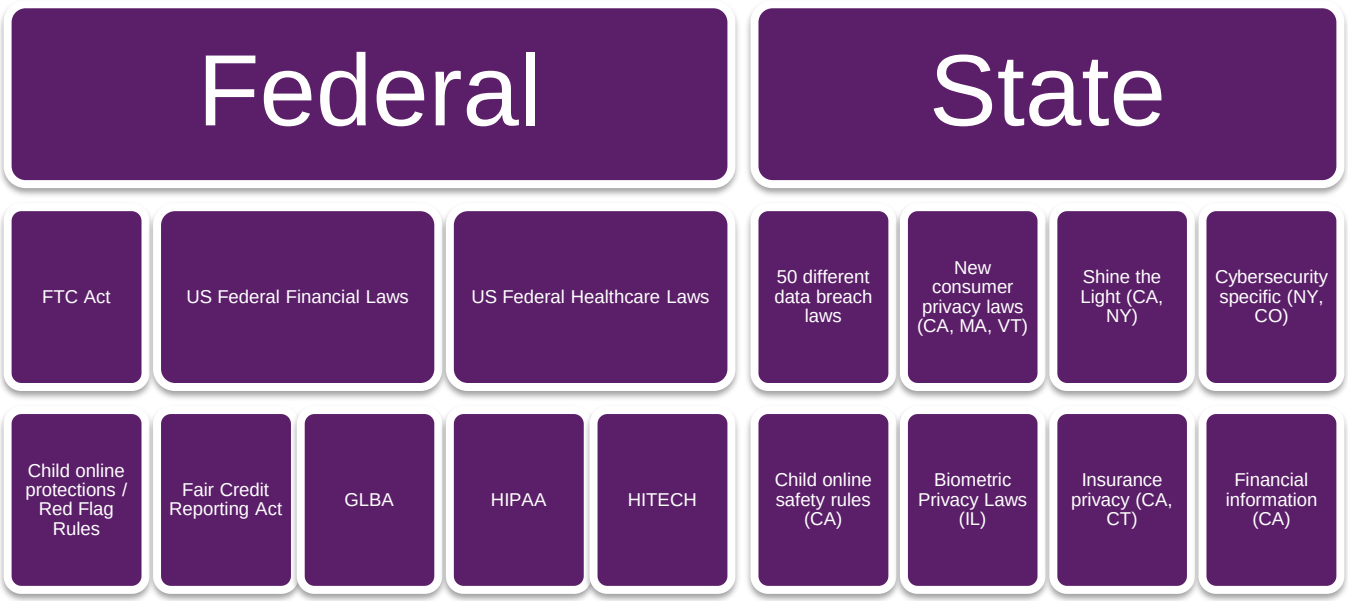
Data Privacy and Security

Getting the terminology right

- **Data privacy**. The privacy rights attached by law to the data and information your enterprise holds.
- **Data security**. The security controls necessary, as prescribed by law and necessity, to secure the private data your enterprise holds.
- **Data subjects**. The persons to whom data belongs.
- **Personal information (or personally identifiable information)**. This is information that can be used to reasonably identify a person or entity.
- **Non-personal information**. Personal information that is publically available, or non-personal information.
- The concepts of **data privacy** and **data security** are interrelated. Failure to recognize the adequate privacy controls around data can lead to **significant financial and reputational fallout**.

Cyber Ethics

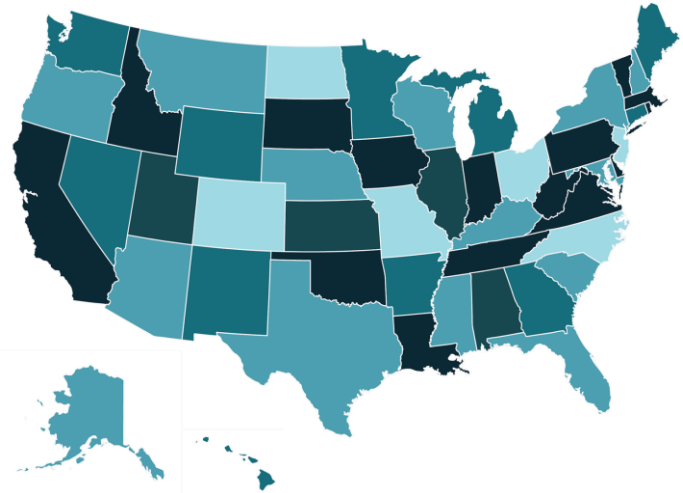
Overview Of U.S. Regulatory Landscape On Privacy



US Data Privacy

Data Breach Law Complications

- All 50 states have different laws
- Varying definitions of data elements
- Paper v. electronic
- Breach exceptions
- Risk of harm
- Notification: individual, State AG, consumer agency
- Notification timelines: 14 days, 30 days, 45 days
- Notification content requirements



US Data Privacy

New State Consumer Privacy Laws Will Impact Employees

California Consumer Privacy Act (CCPA)

- Passed June 2018, effective January 1, 2020
- Introduces broad new rights to “consumers” to request disclosure, deletion, and to opt-out of sales of “personal information”
- Introduces new business obligations of disclosure, privacy policy revisions, and handling of consumer requests
- Attorney General regulatory enforcement carries significant penalties (no cap)
- Private right of action (currently limited, could be expanded) (statutory and actual damages)

State Copy Cat Laws

- **Connecticut** (Act Concerning Consumer Privacy, Raised Bill No. 1108 - 2019)
- **Massachusetts** (An Act Relative To Consumer Data Privacy S. 120 - 2019)
- **Rhode Island** (An Act Relating To Commercial Law - General Regulatory Provisions - Consumer Privacy Protection S 0234 - 2019)

US Data Privacy

New State Biometric Laws Will Impact Employees

Illinois Biometric Privacy Act (BIPA)

- Passed in 2008. Went largely unnoticed until 5 class actions were filed in 2015
- Applies to any business collecting biometric data on Illinois residents (extra-territorial)
- Protects against the collection and use of “biometric identifiers” and “biometric information”
- Imposes specific requirements on covered entities for written policies (external facing), notice, and consent requirements
- No actual harm needed for standing

State Copy Cat Laws

- Texas and Washington have biometric privacy laws in place
- Arizona
- Florida
- Massachusetts
- California (CCPA)

US Data Privacy

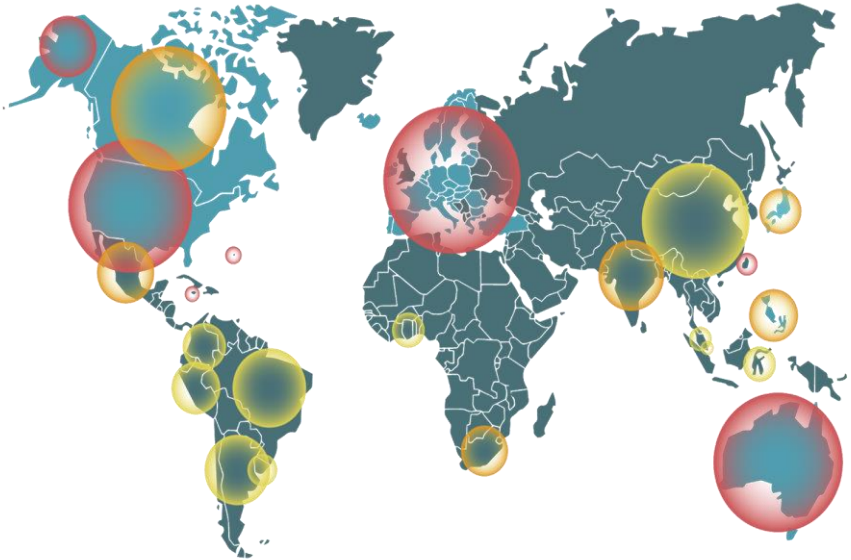
Federal Data Privacy Law Developments

- Drafts are being circulated
- Hearings held
- Intense lobbying efforts by technology industry groups
- Main fight is about preemption. Senator Feinstein - Not unless matches the CCPA
- How to address 50 state patchwork frameworks?

Global Data Privacy Developments

Regulatory Landscape

- EU General Data Protection Regulation (GDPR)
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- Thailand Data Protection Act
- Australia Data Protection Law
- Brazil Data Protection Law
- China Cybersecurity Law
- Vietnam Cybersecurity Law



Cyber Ethics

Overview of ABA Model Rules on Privacy and Cybersecurity

Cyber Ethics

ABA Model Rules and Formal Opinions

Model Rules

- Model Rule 1.6
- Model Rule 1.1

Formal Opinion

- Formal Opinion 99-413
- Formal Opinion 477R
- Formal Opinion 483

Cyber Ethics

Model Rule 1.1: Competence

- **Rule**. A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
- **2012 Comment 8**: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
- **ABA Commission on Ethics 20/20**: The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.

Cyber Ethics

Model Rule 1.6: Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) […]

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

- **2012 Amendment**. Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Cyber Ethics

Formal Ethics Opinion 99-413 (5/10/99)

Protecting the Confidentiality of Unencrypted E-mail A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and a legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.

Cyber Ethics

Formal Ethics Opinion 477R (5/11/17)

Securing Communication of Protected Client Information A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

Cyber Ethics

Formal Ethics Opinion 483 (10/17/18)

Lawyers' Obligations After An Electronic Data Breach Or Cyberattack Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1, and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Cyber Ethics

Takeaways

- **Stay involved, verify practices, train, coordinate efforts, oversee risk**
- Ensure risk is elevated within the enterprise
- Lead a risk assessment
- Verify written information security program is in place
- Train your lawyers and your staff on procedures
- Use technology to your advantage
- Drive a privacy and security-by-design culture that will become sophisticated enough to recognize a threat and report it appropriately

Bio

Team Bio

Peter Stockburger
Senior Managing Associate
San Diego

619.595.8018
peter.stockburger@dentons.com

Peter Stockburger is a senior managing associate at Dentons and is a member of the Firm's global Employment and Labor, Intelligence and Strategic Services, and Privacy and Cybersecurity groups. Peter's practice focuses on the unique intersection between cybersecurity, data privacy, employment law and complex commercial litigation. Peter regularly advises clients on a broad range of cutting-edge legal issues, including cybersecurity resiliency and risk analysis, privacy programs and data protection, cyber gap assessments, workplace disputes, and complex business questions. He also has extensive experience handling a variety of litigation matters, including trade secret and breach of contract disputes, before all level of courts and administrative agencies.

Peter regularly presents in the field of cybersecurity and privacy, including with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in Tallinn, Estonia; the American Society of International Law in Washington, DC; the US Cyber Institute at West Point; ACC; CONNECT; and the San Diego Maritime Alliance. He also publishes extensively in the field, including with NATO CCDCOE and the *American University Journal of International Law*, and was recently invited to participate as an expert in cybersecurity projects commissioned by the University of Leiden in the Netherlands, the University of Exeter in the United Kingdom and NATO CCDCOE.

In addition to his work with the firm, Peter is also an adjunct professor at the University of San Diego School of Law where he teaches in the area of oral advocacy and cyber law. Peter also serves as an advisor to the University of San Diego School of Engineering and Center for Cyber Security Engineering and Technology. He has been recognized as a Rising Star by Southern California *Super Lawyers Magazine* every year since 2015.

Peter also has a dedicated pro bono practice. He has successfully acquired legal status for refugees from Haiti, Mexico and Egypt, and has been the principle author on various amicus briefs filed with the US Supreme Court, the Ninth and Fourth Circuit Courts of Appeal, and the Illinois Supreme Court, including briefs filed in *Gloucester County School Board v. G.G.* (transgender student rights) and *Jennings v. Rodriguez* (immigration detention). For his work, Peter was awarded the Wiley W. Manuel Certificate for Pro Bono Legal Services from the State Bar of California in 2015 and 2017, the Pro Bono Publico Award from Casa Cornelia in 2016, and was named LAF's 2017 OP Appeals Project Volunteer Attorney of the Year in 2017.

Thank you

大成 DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.