PRIVACY & DATA SECURITY 2020:

Mischief Managed: Best Practices in Developing a Cybersecurity Crisis Response Program.

KARIN MCGINNIS AND TODD TAYLOR, MOORE & VAN ALLEN, PLLC; MARY GAMBLE EXECUTIVE VP AND GC, M-PAC, US; JONATHAN WACKROW, MANAGING DIRECTOR, TENEO ADVISORY GROUP

February 13, 2020

Legal Obligations in Data Incident Crisis Response

State Data Security Laws

Currently, at least 23 states have some form of general data security requirement:

- Alabama
- Arkansas
- California
- Colorado
- Connecticut*
- Delaware
- Florida
- Illinois
- Indiana
- Kansas
- Louisiana
- Maryland
- Massachusetts
- Minnesota*
- Nebraska
- Nevada
- New Mexico
- New York (3/21/2020)
- Oregon
- Rhode Island
- Texas
- Utah
- Vermont*

State Data Security Laws

- Most states simply require that the entity implement and maintain reasonable security practices appropriate to the nature of the information to protect from unauthorized access, destruction, use, modification or disclosure.
- Having a data incident response plan arguably is part of "reasonable security measures."
- AL, CT, MA, NV, OR and VT have more robust requirements.

Alabama

Reasonable security measures = security measures practicable to implement and maintain, including consideration of all the following:

- Designation of employee to coordinate security measures to protect against breach;
- Identification of internal and external risks of a breach;
- Adoption of appropriate information safeguards to address identified risks of a breach, and assess the effectiveness of such safeguards;
- Retention of service providers that are contractually required to maintain appropriate safeguards for sensitive personally identifying information;
- *Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information;*
- *Keeping management of the covered entity appropriately informed of the overall status of its security measures.*

Ala. Code 8-38-3 (Section 3)

- Secure disposal of personally identifiable information (Section 10).

Massachusetts Standards for the Protection of Personal Information (*201 CMR §§17.01 & 17.03)*

- Imposes detailed obligations on person or entity that owns or licenses personal information (paper or electronic) of Massachusetts residents to develop, implement, and maintain a comprehensive written information security program.
- These are minimum standards.

Massachusetts Standards for the Protection of Personal Information (*201 CMR §17.03(2)*)

Every information security program shall include :

- Responsible Persons
- Risk Assessment
- Employees/Employer Training
- Discipline
- Limit Access by terminated employees
- Vendor Oversight
- Restrictions on Physical Access
- Monitoring of the program
- Audits
- *Security Incident Documentation* ("document responsive actions taken in connection with any incident involving a breach of security.")

EU General Data Protection Regulation

Article 32 of the **GDPR** requires the following:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate technical and organisational measures*** *to ensure a level of security appropriate to the risk … account shall be taken in particular of the risks that are presented by processing … which could lead to physical, material or non-material damage."*

GDPR, Art. 32

- Measures to ensure an appropriate level of security include:
  - Encryption: the pseudonymisation and encryption of personal data;
  - Systems: the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - ***Restoration: the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;***
  - Auditing: a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

  GDPR, Art. 32(1)(a)

NY Dept of Financial Services (NY DFS) Cybersecurity Regulations (23 NYCRR Part 500)

- Effective March 1, 2017.
- Applicable to entities that are subject to licensing by NY DFS.
- Covered entities are required to maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the company's information system.
- Requires procedures and policies to protect information systems and nonpublic information on the systems.

NY DFS Cybersecurity Regulations
(23 NYCRR Part 500)

WISP Components:

- Risk assessment
- *Incident response*
- Info security
- Network and systems security
- Data governance/classification
- Access controls/id management
- Continuity/disaster recovery
- Continuity/disaster recovery
- Systems/network monitoring
- Physical security
- Vendor management
- Data disposal

NY DFS Cybersecurity Regulations (23 NYCRR 500.16)

Written incident response plan must address:

- the internal processes for responding to a Cybersecurity Event;
- the goals of the incident response plan;
- the definition of clear roles, responsibilities and levels of decision-making authority;
- external and internal communications and information sharing;
- identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Gramm Leach Bliley

Financial institutions

- *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice *available at* **12 CFR PART 30 APPENDIX B**
- **"**Manage and Control Risk. Each national bank or Federal savings association shall:**…. g. Response programs** that specify actions to be taken when the national bank or Federal savings association suspects or detects that **unauthorized** individuals have gained **access** to **customer information** systems, including appropriate reports to regulatory and law enforcement agencies."

PCI-DSS

- Requirements Imposed by Major Card Brands with regards to protection of Cardholder Data.
- Applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers.
- *Requires incident response plan.*

HIPAA

- *Requires security incident procedures*. 45 CFR 164.308(a)(6)(i).
- Security incident procedures. Implement policies and procedures to address security incidents. (ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
- Security incident is defined at 45 CFR 164.304: Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Ohio

Ohio Rev. Code Ann. § 1354.03(D).

- Ohio Data Protection Act: Compliance with cybersecurity program is an affirmative defense to tort action in Ohio alleging that failure to implement reasonable information security controls caused a data breach.
- The cybersecurity program must reasonably confirm to one or more specific industry recognized cybersecurity frameworks (i.e., NIST, FedRAMP), PCI-DSS, or existing federal or state laws that already apply to the entity (for example HIPAA or GLBA).
- https://www.nist.gov/cyberframework/respond

Privilege in Data Incident Crisis Response

Attorney Client Privilege/Work Product

- ***In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1244 (D. Or. 2017)**.
- **Data breach notices** not protected by privilege unless contains edits seeking or containing legal advice.
- **Press releases** "Public relations work is generally treated as business strategy, rather than a legal one, and is not protected as work product…it is not enough to show merely that the material was prepared at the behest of a lawyer or was provided to a lawyer"
- Nor is an attorney's own work subject to protection if the work is intended for public relations or other business purposes rather than litigation; "delegating business functions to counsel to oversee does not provide work-product protection to the materials created for those business functions."
- **Third party forensic or other services** not protected by privilege or work product if under an agreement with client in ordinary course, even if counsel later assumes the agreement.
- Having a data incident response plan can ensure right process is followed to increase ability to claim privilege.

Attorney- Client Privilege (Upjohn)

- Recommended for all interviews by counsel.
- Also consider NRLB and KBR
  - Obama Administration NLRB–The company cannot prohibit a nonsupervisory employee from discussing with others if necessary, to exercise rights to engage in concerted activity under the National Labor Relations Act.
  - Trump Administration NLRB—Recent about face. Employers can require confidentiality by nonsupervisory employees *during* investigations if company has legitimate justifications for requiring confidentiality (balancing test).
  - Next Administration NLRB--???
  - KBR– SEC Rule 21F-17: "No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications."

Upjohn example—Supervisory Employees

- "I am an attorney for the Company and am representing the Company, not you individually. Your communications with me are protected by the attorney-client privilege. But the attorney–client privilege belongs solely to The Company, not you. That means that The Company alone may elect to waive the attorney-client privilege and reveal our discussion to third parties. The Company alone may decide to waive the privilege and disclose this discussion to such third parties as federal or state agencies, at its sole discretion, and without notifying you.
- In order for this discussion to be subject to the privilege, it must be kept in confidence. In other words, with the exception of your own attorney, you may not disclose the substance of this interview to any third party, including other employees or anyone outside of the company. You may discuss the facts of what happened, but you may not discuss *this* discussion.
- To be clear, nothing prohibits you from reporting a violation or possible violation of state or federal law or regulation to any governmental agency or entity **[for public companies list specifically "including but not limited to the Department of Justice, the Securities and Exchange Commission, Congress and any agency Inspector General"]**, or from making disclosures that are protected under the whistleblowing provisions of applicable state or federal law or regulation.
- Do you have any questions? Are you willing to proceed?

Upjohn example—Nonsupervisors (Obama Era NLRB)

- I am an attorney for the Company and am representing the Company, not you individually. Your communications with me are protected by the attorney-client privilege. But the attorney–client privilege belongs solely to the Company, not you. That means that the Company alone may elect to waive the attorney-client privilege and reveal our discussion to third parties. The Company alone may decide to waive the privilege and disclose this discussion to such third parties as federal or state agencies, at its sole discretion, and without notifying you.
- This is a confidential investigation, and your cooperation is required to conduct a thorough investigation. To maintain the integrity of the investigation, the disclosure of information is limited to those with a bona fide need to know, and any information provided will be maintained as confidential except on a need to know basis or if further action is needed requiring disclosure. You can assist in ensuring confidentiality and preserve the integrity of the investigation by not discussing the investigation with others.
- Further, nothing prohibits you from reporting a violation or possible violation of state or federal law or regulation to any governmental agency or entity **[for public companies list specifically "including but not limited to the Department of Justice, the Securities and Exchange Commission, Congress and any agency Inspector General"]**, or from making disclosures that are protected under the whistleblowing provisions of applicable state or federal law or regulation.
- Do you have any questions? Are you willing to proceed?

Role of Law Enforcement; Before, During and After a Data Incident

"Every cyber breach begins and ends in the General Counsels office."
N. MacDonnell Ulsch

<u>In Preparation</u>

- Liaise with Law Enforcement
  - Local, USSS, FBI, Cybersecurity and Communications Integration Cell
  - Bi-directional relationships
- Retain external Cybersecurity firm
- Define Crisis vs Incident
- Develop and Exercise Crisis Response Plan
- Engage stakeholders

<u>In Response</u>

- Engage Legal counsel
  - Internal / External
- Contact Law Enforcement
  - Understand their role
- Engage Cybersecurity firm
  - Preserve evidence
- Maintain System Logs
  - Chain of custody - forensic link
- Engage IRP
  - "Do no harm"

<u>In Repair</u>

- Continue LE Engagement
  - Post incident reporting
  - Criminal inv.
- Communications with internal & external stakeholders
- 3rd party forensic autopsy
  - Share w/law enforcement
- Transparency

Incident Response When Notifying Law Enforcement

Step #1. Knowing who to involve in your initial response

- Legal counsel, HR, corporate security, IT security, technical professionals (3rd Party forensic responders), communications team, & law enforcement

Step #2. Containing the problem while investigating the incident

- A data breach contains three (3) basic components
  - How did they get in?
  - How did they move through your network and what did they take or alter?
  - How did they exit your system?

Step #3. Collecting and reporting the facts.

- The response team must:
  - Control physical access to computers and network components
  - Log and report the sequence of events or incidents
  - Preserve all evidence and maintain a chain-of-custody

Role of General Counsel

- **Prepare before a crisis hits – create a response plan NOW!**
  - What types of potential crises face your company? What is the best response plan for each situation?
- **Response Management**
  - In high stress situations, clients (the company) look to attorneys for comfort, guidance, and answers.
- **What's the Plan? - Prepare and Implement Action Plan.**
  - Prepare and implement an action plan; communicate this plan to the parties involved.
- **Who is at the table?**
  - What is the level of engagement for: in-house management team, outside counsel, external crises response team, internal and external investigators?
- **Define roles, responsibilities, and access to information.**
  - Who is in charge? Who is leading the various crisis response components? Mange the flow of information – who has access and what is privileged?
- **Follow up!**
  - Are the parties involved doing their job? Doing it effectively? Have new issues emerged?
- **Post-event debrief and adjustments to plan**
  - How effective was the crisis response? Is there any potential for future fallout? Can it still be mitigated? How can the plan be improved for next time?

Panel

- KARIN MCGINNIS, MOORE & VAN ALLEN
  - KARINMCGINNIS@MVALAW.COM
- TODD TAYLOR, MOORE & VAN ALLEN
  - TODDTAYLOR@MVALAW.COM
- MARY GAMBLE, EXECUTIVE VP AND GC, M-PAC
  - M.GAMBLE@MPAC.COM
- JONATHAN WACKROW, MANAGING DIRECTOR, TENEO ADVISORY GROUP
  - JONATHAN.WACKROW@TENEO.COM

Questions

KARIN M. MCGINNIS

MEMBER

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

CHARLOTTE

TEL: (704) 331-1078
FAX: (704) 378-2078

karinmcginnis@mvalaw.com

PRACTICE AREAS

- Employment & ERISA Litigation
- Employment & Labor
- Employment & Noncompetition Agreements & Trade Secrets Protection
- ERISA & Benefits
- Financial Regulatory Advice and Response
- Global Services
- Litigation
- North Carolina Business Court Litigation
- Privacy & Data Security
- Trade Secrets Litigation
- Wage & Hour Compliance & Litigation

EDUCATION

- B.S., East Carolina University, 1989
- J.D., University of North Carolina at Chapel Hill, 1992, with high honors; Order of the Coif; North Carolina Law Review Staff, 1990; Senior Staff, 1991

Privacy & Data Security

With two decades of experience as a practicing attorney, Karin McGinnis, CIPP US, has handled a wide variety of privacy and data security matters for her clients, with a special emphasis on privacy and data security issues in the workplace. Recognized by her peers as a Martindale Hubble AV Preeminent and among the North Carolina Legal Elite and Super Lawyers, Ms. McGinnis is known as a true business partner when litigating and providing counsel to her clients.

She has assisted clients with privacy and data security issues internationally, including compliance with GDPR, an international ethics hotline, international data transfers, and data breaches affecting consumers overseas. Ms. McGinnis also has experience drafting record retention, Bring Your Own Device ("BYOD"), and employee mobile device policies and programs in diverse industries, as well as PCI-DSS issues.

Ms. McGinnis' privacy and data security experience includes counseling and litigation regarding misappropriation of trade secrets, violation of the Computer Fraud and Abuse Act and state computer trespass laws, and common law privacy torts. Her litigation experience also includes HIPAA privacy issues, discovery challenges posed by the Stored Communications Act, privacy of consumer financial information under Gramm-Leach-Bliley, and confidentiality rights concerning mental health consumers. She also has successfully negotiated and advised clients in responding TCPA claims.

Ms. McGinnis also handles data breach matters in the U.S. and internationally for her clients and has worked with the USSS and the FBI in investigating potential cyber-crime and data breaches. She has assisted clients with drafting and creating data breach

CONTINUED

BAR & COURT ADMISSIONS

- North Carolina, 1992
- United States District Court Middle District of North Carolina, 1993
- United States District Court Eastern District of North Carolina, 1993
- United States District Court Western District of North Carolina, 1992
- United States Court of Appeals for the Fourth Circuit, 1994

KARIN M. MCGINNIS

procedures, FACTA Red Flag policies and procedures, online privacy policies, CCPA compliance, GLBA compliance, data security plans, data security provisions in vendor agreements, and employee data security training.

In addition, Ms. McGinnis frequently advises clients and drafts policies and agreements in connection with employee monitoring, social media, the Electronic Communications Privacy Act, limitations imposed by the National Labor Relations Act on employee confidentiality and social media policies and agreements, drug testing, the Genetic Information Nondiscrimination Act ("GINA"), the Americans with Disabilities Act Amendments Act (ADAAA), the Fair Credit Reporting Act, the CAN-SPAM Act, and protection of private personnel information under state law.

In the age of increasing commoditization of legal services, from off-the-shelf policies to one-size-fits-all agreements, Ms. McGinnis knows that no two clients' needs are alike, and she works to achieve results that best fit each client's culture, resources and goals.

OF NOTE

- Certified Information Privacy Professional/US (CIPP/US), International Association of Privacy Professionals
- Certified Privacy and Data Security Specialist, North Carolina State Bar
- Member, North Carolina State Bar Specialization Committee for Privacy and Data Security, 2018-2019
- 2018 Women in Business Award Winner, presented by the *Charlotte Business Journal*
- Included in *Chambers* Partners USA in North Carolina - Labor & Employment, 2014-2019
- Selected for inclusion to the "Top 50" list of Women North Carolina *Super Lawyers*, 2020
- Selected for inclusion to the North Carolina *Super Lawyers* list in 2015-2020 for Employment & Labor
- Named among The Best Lawyers in America for Employment Law - Management, 2019-2020

CONTINUED

KARIN M. MCGINNIS

- Named among The Best Lawyers in America for ERISA, 2016-2018
- *Business North Carolina*'s Legal Elite, 2005, 2008-2014, 2017-2020
- Recognized by *Benchmark Litigation* as a Labor & Employment Star-South, 2019 and Labor & Employment Star, 2020
- 2014 ATHENA Leadership Awards, Corporate Nominee
- Leader in the Law, *North Carolina Lawyers Weekly*, 2012
- Business Leader Media Award Women Extraordinaire, 2010
- Martindale Hubble Rated AV Preeminent
- Guest Lecturer, Wake Forest Law School, Law and Technology Class (August 26, 2019)
- Presenter, Globalaw's 2018 European Regional Seminar, Rome, Italy (April 19, 2018)
- Co-Presenter, "The EU General Data Protection Regulation: A Primer for U.S. Companies," Association of Corporate Counsel- Charlotte Chapter (February 21, 2018)
- Author, "New Data Breach Rulings — 4th Circ. Vs. 3rd Circ.," Law360 (February 9, 2017)
- Author, "Expect More Privacy Challenges This Year," Legaltech News (April 2016)
- Co-Presenter, "Cyber War Games," Association of Corporate Counsel- South Carolina Chapter Annual Meeting (November 10, 2015)
- Co-Presenter, "Protecting Information While Employing Workers Overseas," Globalaw Client Seminar (October 23, 2015)
- Co-Author, "Efforts to Fix Data Security Flaws Carry Weight with FTC," National Law Journal (February 2015)
- Author, "The Ever Expanding Scope of Employee Privacy Protections," ACC Charlotte Chapter Newsletter (December 2014)
- Co-Author, "Cybersecurity Special Report: Trade Commission Takes Line on Data Security," National Law Journal (November 2014)
- Co-Presenter, "Privacy and Social Media in the Workplace," MVA Privacy & Data Security Seminar Series (May 29, 2014)

CONTINUED

KARIN M. MCGINNIS

- Author, “Social Media- Love it or Leave it?” Business North Carolina (May 2014)
- Co-Presenter, “Preventing and Responding to a Cybersecurity Event from the Legal and Technical Perspectives: NIST Cybersecurity Framework,” MVA Privacy & Data Security Seminar Series (March 27, 2014)
- Co-Presenter, “Social Media Strategies and Risks,” Association of Corporate Counsel-Charlotte Chapter (February 5, 2014)
- Co-Presenter, “Privacy and Social Media in the Workplace: What U.S. and E.U. Employers Need to Know,” Globalaw Webinar (December 9, 2013)
- Author, "5 Ways to Reduce Liability in Hiring a Rival’s Employee," Corporate Counsel (October 10, 2013)
- Author, "Look Before You Leap: Employee 'Bring Your Own Device' Programs," Corporate Board Member (January 2013)
- "Legal Issues Associated with Corporate Bring Your Own Device Programs," JP Morgan Chase, New York, New York (December 6, 2012)
- Co-Author, "4 Tips for Drafting an Enforceable Employment Covenant," Inside Counsel (August 13, 2012)
- Co-Author, "3 Ways to Avoid Problems with Ex-Employees," Inside Counsel (July 30, 2012)
- Co-author, "7 Ways to Avoid Trouble with the EEOC," Inside Counsel (July 16, 2012)
- Co-author, "5 Ways to Avoid Trouble with the Department of Labor," Inside Counsel (July 2, 2012)
- Co-author, "Avoid Trouble with the NLRB," Inside Counsel (June 18, 2012)
- Co-author, "14 Tips for Smoother Hiring, Employment and Termination," Inside Counsel (June 4, 2012)
- Lead counsel for the plaintiff, "Mock Trial: Hostile Work Environment" presentation for Society of Human Resource Management (Charlotte, NC chapter) (October 11, 2010)
- Co-Author, "Feds ready to crack down on employee classification" for the Charlotte Business Journal (April 16, 2010)

CONTINUED

KARIN M. MCGINNIS

- Presented "Top 10 HR Priorities for 2010" at The Employer's Association (February, 19, 2010)
- Author, "Employee Leave: The Essentials Behind What You Have to Do and What You Should Do to Retain Top Management," chapter in ExecBlueprints series
- Author, "Helping Businesses Stay Compliant," chapter in Inside the Minds: Labor and Employment Litigation Strategies
- Chair, Board of Directors and Personnel Committee Chair, Second Harvest Food Bank of the Metrolinas
- Pro bono counsel assisting nonprofit organizations with employment law issues
- Past Chair, Young Lawyers Division of the North Carolina Bar Association
- Served as guardian ad litem for the Children's Law Center
- Serves as pro bono domestic violence counsel
- Former member, Film Advisory Board of the Carolinas Partnership
- Former Board of Directors member, Volunteer Lawyers for the Arts
- Graduate, Charlotte Chamber of Commerce Leadership School
- Named to the Access to Justice Pro Bono Partners 2013 Pro Bono Honor Roll by Legal Services of Southern Piedmont, Legal Aid of North Carolina–Charlotte, and Council for Children's Rights

PROFESSIONAL AFFILIATIONS

- International Association of Privacy Professionals
- American Bar Association: Labor and Employment and Litigation Sections; Women Advocates Committee
- North Carolina Bar Association: Labor and Employment and Litigation Sections
- Young Lawyers Division, Secretary, Past Division Director for Service to the Bar, Long Range Planning Committee, Past Division Director for Service to the Public, Chair-Elect, 2000-2001; Chair 2001-2002
- North Carolina Bar Association: Board of Governors, 2001-2002; Nominations Committee 2002-2003

CONTINUED

KARIN M. MCGINNIS

- North Carolina Bar Association: Lawyer Effectiveness and Quality of Life Committee 2006-2019
- North Carolina Bar Association: President's 4-All Task Force, 2007-2008
- North Carolina Bar Association Pro Bono Task Force

Moore&VanAllen

PRACTICE AREAS

- Commercial & Technology Transactions
- Financial Regulatory Advice and Response
- Global Services
- Intellectual Property
- Privacy & Data Security

EDUCATION

- J.D., University of North Carolina School of Law, 1995, honors
- B.A., North Carolina State University, 1992, summa cum laude

BAR & COURT ADMISSIONS

- North Carolina, 1995

OTHER AREAS OF LAW

- Outsourcing
- Cross-Border Transactions
- Technology Licensing
- E-Commerce Transactions
- Mergers & Acquisitions
- Joint Ventures
- Corporate Law
- Supply Chain Matters

TODD C. TAYLOR

MEMBER

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

CHARLOTTE

TEL: (704) 331-1112
FAX: (704) 409-5611

toddtaylor@mvalaw.com

Todd Taylor serves as a Member and co-leader of Moore & Van Allen's Commercial & Technology Transactions practice group, as well as its Privacy & Data Security group. Taylor focuses his practice on data privacy and security, licensing, technology, supply chain and commercial transactional matters.

Before joining Moore & Van Allen, Taylor served as an in-house attorney at Bank of America, where he worked extensively on various technology licensing, supply chain, cross-border and third party servicing arrangements.

SPEAKING ENGAGEMENTS

- "Introduction to Legal Issues in Outsourcing," Mecklenburg County Bar Association, Charlotte, North Carolina, February 11, 2010
- "IP Trademark, Copyright & Licensing Counsel Forum," an *ALM/Corporate Counsel Event,* The Harvard Club, New York City, September 15, 2011
- "Overview of Third-Party Contracting and Outsourcing," National Business Institute, Charlotte, North Carolina, December 8, 2011
- "Outsourcing and Offshoring," Mecklenburg County Bar Association, Charlotte, North Carolina, February 2, 2012
- "Legal Issues Associated with Corporate Bring Your Own Device Programs," JP Morgan Chase, New York, New York, December 6, 2012
- "Addressing Risks in Contracting with Parties in Emerging Markets," Association of Corporate Counsel's Contracts & IP Symposium, Charlotte, North Carolina, November 1, 2013

CONTINUED

TODD C. TAYLOR

- "Privacy & Social Media in the Workplace," *Globalaw* webinar, December 9, 2013
- "Social Media- Strategies and Risks," Association of Corporate Counsel Charlotte Chapter, February 5, 2014
- "How to Navigate the Data Breach Storm: Identifying the Risks and Managing the Aftermath," CommercialLawWebAdvisor webinar, January 15, 2015
- "Export/Import Issues & Data Movement Concerns in Cross-Border Transactions," Association of Corporate Counsel Charlotte Chapter, July 23, 2015
- "Effective Data Security Management: Keeping Your Data Protected in the Cloud," The Knowledge Group, March 22, 2016
- "Data Breaches And Cyber Security – Are You Ready?," ABA/Young Lawyers' Division 2016 Fall Conference, October 20, 2016
- "Technology & Data Issues in Contracts: Crafting Intellectual Property Licensing Related Provisions & Information Sharing and Security Related Provisions," Association of Corporate Counsel Charlotte Chapter, February 15, 2017
- "The EU General Data Protection Regulation: A Primer for U.S. Companies," Association of Corporate Counsel Charlotte Chapter, February 21, 2018
- "The Digital and Privacy Law Revolution: The Impact of Privacy Law and the Cloud on Business," ACC South Carolina Annual Meeting, September 28, 2018

PUBLICATIONS

- "A collision of rules in the evolving world of online banking," *The Hill*, January 12, 2017
- "New York's proposed cyber-security compliance challenge," *Compliance Week*, December 21, 2016
- "New York's Proposed Cybersecurity Regulations: An Old Path Or a New Trail?," *Bloomberg Law Reports- Banking*, November 22, 2016
- "Proposed Global Online Freedom Act Could Impact Supply Chains, Outsourcing Efforts and Foreign Operations of U.S. and Multinational Companies," *Bloomberg Law Reports – Technology Law*, January 18, 2012

CONTINUED

TODD C. TAYLOR

- "Purging Slavery from California's Supply Chain," *Law360*, February 7, 2012
- "Corporate Cybersecurity: Emerging Threats & Recent Developments," *Corporate Board Member*, 2nd Quarter 2012 edition
- "US Employment Woes Slow Visas for Foreign Workers," *Charlotte Business Journal*, May 18, 2012
- "An Analysis of Proposed Federal Cybersecurity Legislation," *Corporate Counsel,* September 17, 2012
- "Blogger's liability for third-party comments and content: A growing legal threat for bloggers or plaintiffs' lingering ignorance of the law?" *Westlaw Journal— Computer & Internet,* November 30, 2012
- "Technology: 4 important issues to address in the brave new world of BYOD programs," *InsideCounsel,* November 30, 2012
- "Defending against cyber-attacks," *InsideCounsel*, December 14, 2012
- "The biggest social media lesson of 2012," *InsideCounsel*, December 28, 2012
- "Navigating the export control maze," *InsideCounsel*, January 11, 2013
- "Don't let the cloud services Grinch steal your Christmas," *InsideCounsel*, January 25, 2013
- "Ensuring ownership of contractor-created technology and other works," *InsideCounsel*, February 8, 2013
- "Social Media in the workplace: The impact of recent NLRB rulings," *Westlaw Journal Computer & Internet*, May 3, 2013
- "Social Media and the Stored Communications Act: Does a 1986 Law Protect Timelines and Tweets?" *Bloomberg Social Media Law & Policy Report*, November 26, 2013
- "Can Using Facebook Be a Firing Offense?" *The Corporate Counselor*, December 2013
- "3 data security best practices learned from FTC enforcement actions," *InsideCounsel*, June 2, 2014
- "EU-U.S. Safe Harbor agreement heading for troubled water?" *InsideCounsel*, July 17, 2014

CONTINUED

TODD C. TAYLOR

OF NOTE

- Selected for inclusion in *IAM Patent 1000: The World's Leading Patent Practitioners*, 2019
- Certified Information Privacy Professional/US (CIPP/US), International Association of Privacy Professionals
- Theatre Charlotte, Past Board Member
- Graduate of Mecklenburg County Bar Leadership School
- Graduate of Mecklenburg County Civic 101 Program
- Past Pack Treasurer/Assistant Den Leader for Cub Scout Pack 24/Mecklenburg Boy Scouts Apache Counsel
- Junior Achievement of the Central Carolinas, Past Board Member
- Charlotte Mecklenburg Police Athletic League, Past Board Member

PROFESSIONAL AFFILIATIONS

- Member of the International Association of Privacy Professionals
- Former Law Clerk to Judges Charles Poston and Lydia Taylor, Norfolk Circuit Court, Norfolk, Virginia
- Mecklenburg County Bar Association
- North Carolina Bar Association
- North Carolina State Bar
- American Bar Association

Mary Gamble, Executive VP and GC, M-Pac
m.gamble@mpac.com

Mary Gamble earned her Bachelor of Arts from Clemson University before continuing her educational pursuits at Quinnipiac University, where she earned both a Juris Doctor and Master of Business Administration degree. During law school Mary completed an International Law program at the University of Florence in Italy, clerked at the General Counsel's Office for the Executive Office of United States Attorneys, and worked in the International Law and Intellectual Property legal departments for one of the world largest fast-food franchises at its world headquarters in Connecticut as well as in a position she created working out of their Amsterdam office.

Following graduation, Ms. Gamble has gone on to practice law for a renowned Charlotte, North Carolina law firm and is licensed to practice law in both New York and North Carolina. She is a rising star in the legal profession and expanded her talents by stepping into the security industry as Executive Vice President and General Counsel for m_PAC, where she has worked since the company expanded into the USA in 2012. She is actively involved with the local Bar Association, Association for Corporate Counsel, and ASIS as a member of the Young Professionals Council and the Women in Security Counsel where she serves on Council's Board.

Jonathan Wackrow, Managing Director, Teneo Advisory Group

jonathan.wackrow@teneo.com

Jonathan Wackrow is a Managing Director with Teneo. In this role, he leads strategic and crisis communications campaigns and advises CEOs, management teams, and Boards on issues relating to security risk management, crisis preparedness, planning, management and response.

Jonathan is an exclusive Law Enforcement Analyst for CNN; providing on-air analysis of law enforcement, safety, and security matters for domestic and international events.

Prior to joining Teneo, Jonathan was the Executive Director of RANE Corp's Advisory Group. In that capacity, he advised leading corporations on enterprise security risk management, critical infrastructure protection, physical security, executive protection and crisis management procedures. He is a nationally recognized expert on event security policy and procedures. He regularly presents at the annual conferences for the Event Services Professionals Association, the Event Industry Council and Meeting Planners International.

Jonathan spent a majority of his professional career in the United States Secret Service, serving as a criminal investigator in New York City and served on the Presidential Protection Division in Washington, DC. While assigned to the President's detail, he managed numerous high-level security operations both in the United States and abroad while assigned to the protection of the President, First Lady of the United States.

Jonathan is a graduate of Loyola University in Baltimore, Maryland, the Federal Law Enforcement Training Center and the United States Secret Service Academy.