THEBECKAGEFIRM

WOMAN AND VETERAN OWNED **DATA SECURITY & PRIVACY LAW FIRM**

UB Law GOLD Group
Cybersecurity and Ethics CLE

Attorney Advertising: Prior Results Do Not Guarantee Similar Outcomes

Jennifer A. Beckage, Esq., CIPP/US, CIPP/E is a former tech business owner, and public company executive overseeing tech products. Jen has received numerous peer - nominated recognition, including (for the last 6 years) being one of the Top 50 Data Breach Lawyers in the U.S.

Beckage is counsel to some of the globe's largest organizations, brands, not-for-profits, celebrities, high- net-worth individuals, and Fortune 100 Companies. She counsels on space, AI, and other technology and is peer recognized for her data security, privacy and litigation background. She is a peer nominated Best Lawyer in America©, multiple year recipient of SuperLawyer© designation for technology and litigation.

Beckage received MIT "Artificial Intelligence: Implications for Business Strategy" Certification and taught masters data scientists at the State University of New York (SUNY).

Beckage is a Certified Information Privacy Professional, United States (CIPP/US) and Certified Information Privacy Professional, Europe (CIPP/E). She also received MIT "Artificial Intelligence: Implications for Business Strategy" Certification in 2020.

Prior to her legal career, Beckage owned and led technology companies, one of which she helped lead to the sale to a publicly traded company.

JENNIFER A. BECKAGE

ESQ., CIPP/US, CIPP/E

Managing Director

OVERVIEW

THEBECKAGEFIRM

The Beckage Firm is a well-known and respected boutique data security and privacy law firm supporting organizations of all sizes.

Data Security	Data Privacy	Incident Response	Litigation / Regulatory

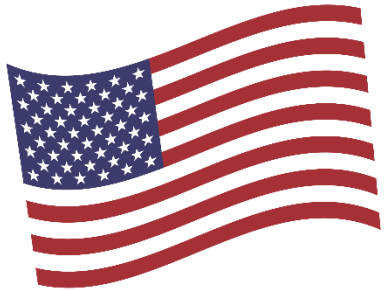
The Beckage Firm includes lawyers who are also technologists cited by international media, speak globally on artificial intelligence (AI), space, crypto, quantum, blockchain, emerging tech, and data security and privacy matters.

WE ARE AMONG THE FIRST TO:

- *Defend nationwide data breaches*
- *Defend putative class actions in response to data breaches*
- *Incorporate AI technologies in Incident Response (IR) and data practices to reduce cost*
- *Defend clients among the largest data privacy regulatory matters*
- *Defend clients involved in the world's largest historical data privacy breach*
- *Draft among the first AI policies and practices*

REAL EXPERIENCE IN PRACTICE

- *Former Public Company Executive*
- *Former Military Leaders*
- *Owners of Tech Companies*
- *General Counsel for Health Organizations*
- *Numerous Security, Privacy, and AI Certifications*



Our team has a wide range of designations including:
Security+, CAPM, CASP, CISM, CISSP, CompTIA Security+, Computing of Elements (UT), Microsoft AZ-900: Microsoft Azure Fundamentals, Microsoft SC-900: Microsoft Security, Compliance, and Identity.

AGENDA

1. Overview of CLE – Cybersecurity & Ethics Requirement in NY
2. Data Security v. Data Privacy
3. Data Security Laws
    a. Federal Legal Requirements
    b. PCI DSS
4. Data Privacy Laws
    a. International
    b. Federal & State
5. Legal Ethical Requirements
    a. Duty of Confidentiality
    b. Duty to Supervise
    c. Duty of Competence
    d. Ethical Decisions
    e. State Ethical Decisions Addressing the Use of AI
6. Q&A

THE BECKAGE FIRM

WOMAN AND VETERAN OWNED **DATA SECURITY & PRIVACY LAW FIRM**

NY REQUIREMENT

22 NYCRR § 1500.2 Definitions

(h) Cybersecurity, Privacy and Data Protection

(1) Cybersecurity, Privacy and Data Protection- Ethics must relate to lawyers' ethical obligations and professional responsibilities regarding the protection of electronic data and communication and may include, among other things: sources of lawyers' ethical obligations and professional responsibilities and their application to electronic data and communication; protection of confidential, privileged and proprietary client and law office data and communication; client counseling and consent regarding electronic data, communication and storage protection policies, protocols, risks and privacy implications; security issues related to the protection of escrow funds; inadvertent or unauthorized electronic disclosure of confidential information, including through social media, data breaches and cyberattacks; and supervision of employees, vendors and third parties as it relates to electronic data and communication. **[effective January 1, 2023]**

(2) Cybersecurity, Privacy and Data Protection-General must relate to the practice of law and may include, among other things, technological aspects of protecting client and law office electronic data and communication (including sending, receiving and storing electronic information; cybersecurity features of technology used; network, hardware, software and mobile device security; preventing, mitigating, and responding to cybersecurity threats, cyberattacks and data breaches); vetting and assessing vendors and other third parties relating to policies, protocols and practices on protecting electronic data and communication; applicable laws relating to cybersecurity (including data breach laws) and data privacy; and law office cybersecurity, privacy and data protection policies and protocols. **[effective January 1, 2023]**

THE BECKAGE FIRM

WOMAN AND VETERAN OWNED DATA SECURITY & PRIVACY LAW FIRM

DATA SECURITY V. PRIVACY

Let's start at the beginning...

The Difference between:

- Data Security
- Data Privacy

THE BECKAGE FIRM

WOMAN AND VETERAN OWNED DATA SECURITY & PRIVACY LAW FIRM

DATA SECURITY LAWS

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA")

HIPAA establishes standards and requirements for health care providers, health plans, and health care clearing houses (defined as "Covered Entities") to protect patient information ("Protected Health Information" or "PHI").

"Business Associate" includes: "a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI; a person that offers a personal health record to one or more individuals on behalf of a Covered Entity; or a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate."

The regulations further provide that the responsibilities of Business Associates include "providing records and compliance reports, cooperating with complaint investigations and compliance reviews, and permit access to information."

TELEPHONE CONSUMER PROTECTION ACT ("TCPA")

Requires prior express consent of an individual before the business uses various telemarketing, automated calls, text messages, and faxes, including prerecorded messages.

The TCPA prohibits the use of automated calls or text messages (both broadly interpreted) to telephone numbers on the National Do Not Call Registry, unless the recipient has provided prior express consent to receive such calls or messages. It imposes certain restrictions on the use of prerecorded or artificial voice messages (e.g., used by vendors such as health plans and staffing companies), and requires that certain information be included in all telemarketing calls, such as the identity of the caller and the purpose of the call.

AMERICANS WITH DISABILITIES ACT ("ADA")

This Act requires that "public accommodations," including private company websites and web-based applications, be accessible to individuals with disabilities. This includes providing equal access to information, functionality, and content.

Web Content Accessibility Guidelines ("WCAG") for the standards that an organization should employ to demonstrate reasonable accommodations. WCAG has three conformance level standards, Level AA compliance (the second highest level) is the goal for acceptable compliance. To meet Level AA conformance, the website/app must be usable and understandable for the majority of people with or without disabilities.

CAN-SPAM

Regulates commercial messages including any advertising messages and promotions for services or products.

There are generally seven (7) main requirements to comply with CAN-SPAM:

- Do not use false or misleading header information.
- Do not use deceptive subject lines.
- Identify the message as an ad.
- Tell recipients where you are located.
- Tell recipients how to opt out of receiving future email from you.
- Honor opt-out requests promptly.
- Monitor what others are doing on your behalf.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS ("PCIDSS")

THEBECKAGEFIRM

Global card brand requirement designed to prevent fraud through the increased control of credit card data. While the PCI DSS has no legal authority to compel compliance, it becomes binding when inserted into merchant card processing contracts used by Visa, Mastercard, Discover Financial Services, JCB International, and American Express.

4 Levels:

Level 1: Applies to merchants processing more than six million real-world credit or debit card transactions annually. Level 1 merchants must conduct an internal audit one a year and submit to a PCI scan by an Approved Scanning Vendor one a quarter.
Level 2: Applies to merchants processing one to six million real-world credit or debit card transactions annually. Level 2 merchants are required to complete an assessment one a year using a Self-Assessment Questionnaire and may be required to conduct a quarterly PCI scan.
Level 3: Applies to merchants processing between 20,000 and one million e-commerce transactions annually. Level 3 merchants are required to complete a yearly assessment using the relevant Self-Assessment Questionnaire and may require a quarterly PCI scan.
Level 4: Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. Level 4 merchants are required to complete the Self-Assessment Questionnaire and may be required to complete a quarterly PCI scan.

THE BECKAGE FIRM

WOMAN AND VETERAN OWNED **DATA SECURITY & PRIVACY LAW FIRM**

DATA PRIVACY LAWS

EU/UK GENERAL DATA PROTECTION REGULATION (”GDPR”)

The main principles of the EU GDPR include:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- accountability

CANADIAN PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT ("PIPEDA")

PIPEDA applies to private-sector organizations across Canada that collect, use, or disclose personal information (as defined in the statute) during a commercial activity. The test is whether the organization engaged in commercial activity in Canada. The law defines commercial activity as "…any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

CANADIAN ANTI-SPAM LEGISLATION ("CASL")

CASL regulates sending commercial electronic messages to an electronic address without the recipient's consent or install programs on computers or networks without express consent.

CASL applies to any commercial electronic message sent to an electronic address in Canada. A commercial electronic message is an electronic message, including email or text message, where one of the purposes to encourage the recipient to participate in a commercial activity.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT ("COPPA")

Federal law that prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children under the age of thirteen (13) on the Internet.[12] COPPA applies to operators, defined as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service.

COPPA states that operators of any website or online service directed to children that collects personal information from children are required to:

- Provide notice on the website of what information is collected from children,
- Notice about how the operator uses the collected information,
- Notice of operator's disclosure practices for collected information, and
- Obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.

COPPA further requires that upon request of a parent whose child has provided personal information to that website or online service, operators are required to provide:

- A description of the specific types of personal information collected from the child by that operator,
- The opportunity to refuse to permit the operator's further use, maintenance, or future collection of personal information from that child, and
- Reasonable means for the parent to obtain any personal information collected from that child.

VIDEO PRIVACY PROTECTION ACT ("VPPA")

Regulates the disclosure of personal user information concerning the consumption of online video content, and imposing requirements to obtain consumers consent to such disclosure that is not hidden in an online privacy policy.

Applies to a "video tape service provider," which is an entity that engages in the sale of prerecorded video cassette tapes or similar audio-visual materials.

OVERVIEW OF U.S. STATE PRIVACY LAWS

THEBECKAGEFIRM

Privacy Laws Are Currently In Effect In:

- California
- Virginia
- Colorado
- Connecticut
- Utah

Additional States Have Passed and Signed Into Law Comprehensive Privacy Laws In:

- Iowa
- Indiana
- Tennessee
- Montana
- Texas
- Oregon
- Delaware
- New Jersey

THE BECKAGE FIRM

WOMAN AND VETERAN OWNED DATA SECURITY & PRIVACY LAW FIRM

ETHICAL RULES

ETHICAL DUTY OF CONFIDENTIALITY

Lawyers have an ethical duty to take reasonable steps to safeguard the confidentiality of client data.

Just like with paper, lawyers must work to protect the intangible, electronically stored information in their possession.

Lawyers must take steps to safeguard confidential information against their own inadvertent disclosures and those of others participating in the representation AND act competently to safeguard confidential information against unauthorized access by third parties.

Lawyers must assess whether circumstances warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

ETHICAL DUTY TO SUPERVISE

THEBECKAGEFIRM

Supervising Non-Lawyers or Subordinate Lawyers

Lawyers who do so must keep in mind their obligations to help ensure that internal and external non-lawyer assistants carry out their duties in a manner that is compatible with the lawyer's professional obligations. While lawyers can and should align themselves with experts, Rule 1.1 makes clear that lawyers cannot simply delegate or outsource technology competence. b. Rule 5.3(b): Responsibility Over Non-Lawyers (i.e., Choosing and Supervising Vendors).

A lawyer is responsible for certain conduct of a nonlawyer employed/ retained by or associated with the lawyer. c. Rule 5.3, Comment [3]: "A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client." One such example is using an Internet-based service to store client information.

When using outside services, the lawyer "must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the nonlawyer's work."

When retaining or directing a nonlawyer outside the firm, a lawyer should appropriately communicate directions to give reasonable assurance that the nonlawyer's conduct is compatible with the lawyer'' professional obligations.

ETHICAL DUTY OF COMPETENCE

Ethics rules also require lawyers to have the technological competence.

With respect to cybersecurity, lawyers must have a basic understanding of the technologies they use, and as technology advances, lawyers need to stay current on changes in the way information is maintained, stored, and organized, or associate themselves with people who do to help educate them.

All litigators should understand the electronic discovery rules in relevant jurisdictions.

A lawyer's duty of competence includes keeping up with changes in both areas.

The requirement of technology competence also intersects with a lawyer's duty to safeguard money held in trust.

Reasonableness Standard.

ETHICAL DECISIONS

THEBECKAGEFIRM

N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 940 (2012). "A lawyer may use off-site backup tapes to store confidential client information if the lawyer takes reasonable care to ensure that the storage system, and the arrangements for its use, adequately protect the confidentiality of such information." See also N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 842 (2010) (same principles addressed in determining reasonableness and use of cloud storage); N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1020 (2014). Authorized persons should have access to cloud storage containing confidential information.

N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 842 (2010). Addresses Rule 1.6 and reiterates that an attorney must take reasonable steps to protect confidential information. Reasonable care may include consideration of the following: 1. that there is a way to ensure that the provider has enforceable obligations to preserve confidential information; 2. that there is a method by which to investigate providers' security measures; 3. that the provider employs technology to guard against access to data; and 4. that the provider has the ability to wipe data/move it. See, N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1020 (2014).

N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1019 (2014). In providing lawyers remote access to client files, a law firm must take reasonable steps to protect information, but: "Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients."

Border crossing and keeping data confidential. N.Y. St. Bar Ass'n Comm. on Prof. Ethics Formal Op. 2017-5 (2017). During border searches, confidential information may be on the attorney's electronic devices, which may be searched.

ETHICAL DECISIONS RELATING TO AI

CALIFORNIA

The "Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law," setting initial recommendations of the Committee on Professional Responsibility and Conduct of the California State Bar regarding use of generative AI in practice of law. The guidelines include confidentiality, competence, communication regarding generative use of AI, billing for AI work, candor to the tribunal,, and prohibition on discrimination, harassment, and retaliation.

FLORIDA

Florida Bar Advisory Opinion 24-1 concludes a lawyer may utilize generative artificial intelligence so long as the lawyer can guarantee compliance with the lawyer's ethical obligations including confidentiality, lawyer oversight, legal fees and costs, and lawyer advertising.

THANK YOU / Q&A

Thank you!

THEBECKAGEFIRM

WOMAN AND VETERAN OWNED **DATA SECURITY & PRIVACY LAW FIRM**

Jennifer A. Beckage, Esq., CIPP/US, CIPP/E – jbeckage@thebeckagefirm.com