VORYS

New thinking.
Since 1909.

Beyond the Breach: Data Privacy Challenges and Legal Ethics in 2025

Attorney Professional Conduct Session

Presenters

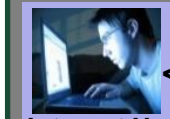
Eric Richardson
513.723.4019
ewrichardson@vorys.com

Brent Craft
513.723.4072
bdcraft@vorys.com

The number of users and methods used to access cyberspace have grown exponentially…

Exponential Growth

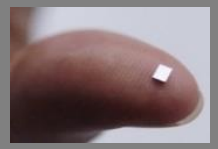
Growth in the developed world exploded over the last 30 years…

	1990	2024
 *Internet Users*	< 1 million	5.5 billion
 Cell Phones	11 million	7.21 billion
 Digital Data	100 Petabytes	Over 149 zettabytes
 Internet Hosts	300,000	Over 1 billion

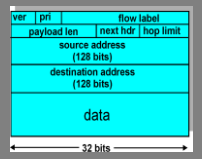
New Technologies

…and will accelerate as a result of new technologies and reduced prices…

$100 laptops



Miniaturized "Smart" Devices



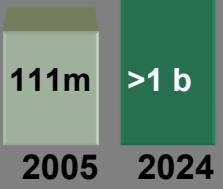
IP v6

Ubiquitous Wireless Networks

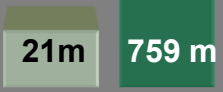
Global Adoption

…fueling the adoption of cyber capabilities in developing countries

Internet Users in China



Internet Users in India



VORYS

…which has transformed business models and driving economic growth

Massive Investment

Industry / Gov't invest $4t in ICT goods and services every year…

$400b

Computers

$360b

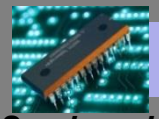
Software

$60b

Servers

$100b

Network Equipment



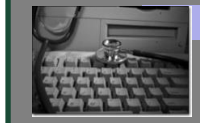
$260b

Semiconductors

Mission Enablement

…These investments have transformed business models and military operations…

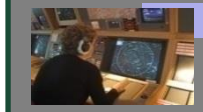
Finance:
$3.2t per day in foreign exchange



Health:
Electronic Health Records

Energy:
300k kilometers of lines carrying 3.8 b kilowatts per year

E-Commerce:
$200b in on-line sales



Air Transportation:
741 million passengers per year

Defense:
Network-Centric Operations

Growing Vulnerabilities

…while exposing substantial vulnerabilities and risks

Hackers steal 40 million credit card numbers

Hackers steal 8.3 million Health Records

Electricity grid in U.S. penetrated by spies

Hackers break into FAA Air Traffic Control Systems

VORYS

In this new environment, the threats are more diverse, increasing in frequency and magnitude of attacks

More Diverse

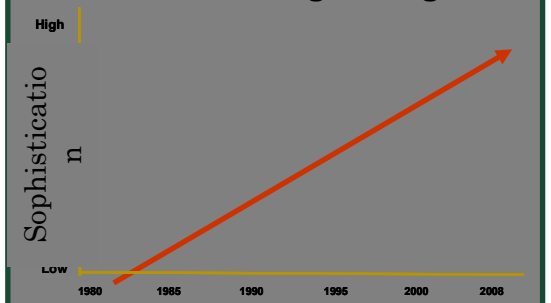
The threats have become more diverse and distributed…

Risks include both malign and benign threats

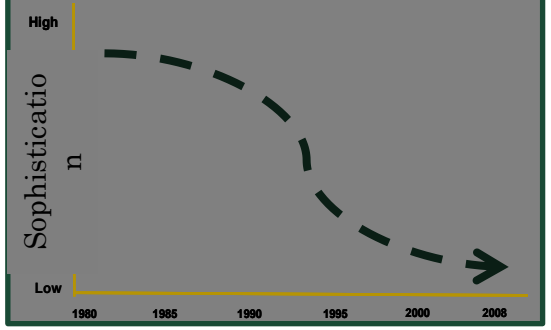
More Capable

… while growing in sophistication with lower barriers to entry

The sophistication of available tools is growing



While the sophistication required of actors is declining



Greater Impact

…increasing the frequency and impact of attacks (2024 statistics)

4,876 CONFIRMED DATA BREACHES

1.7 billion + PEOPLE IMPACTED

$4.88 million = Global Average Total Cost of Data Breach in 2024

$9.36 million = Average Cost of Data Breach in U.S.

VORYS

2024 Statistics

- **4,876** confirmed data breaches in 2024
- **3,158** total compromises
- **211%** increase in victim notices
- Most affected areas include financial services, healthcare, professional services, manufacturing, and education
- Healthcare breach most expensive—average total cost of a breach was $11.45 million in 2024
  - Financial second highest at $6.1 million

2024 Statistics

- 85% of breaches involve external actors
- 68% of data breaches include the “human element”
  - Misusing privileges and using stolen credentials remain top causes
  - Phishing now accounts for **33%** of social-engineering breaches
  - Average time to identify and contain a breach involving human error: **295 days**

2024 Statistics

- What were the primary causes of data breaches in 2024?
  - 42% of breaches resulted from **system intrusion**
  - 33% involved **phishing** or **social engineering**
  - 16% were caused by **stolen credentials**
  - 6% were rooted in **exploiting system vulnerabilities**

2024 Statistics

- Other causes of data breaches included:
  - 8 % – Business Email Compromise
  - 7 % – Accidental data exposure or misconfiguration
  - 3 % – Physical loss / stolen devices
  - 2 % – Insider misuse

2024 Statistics

- Other 2024 data breach statistics:
  - 94% of breaches were **financially motivated**
  - 29% of cybersecurity incidents were **ransomware attacks**
  - Approximately 40% of reported incidents involved **small businesses** (less than 1,000 employees) through:
    - Phishing/social engineering
    - Credential theft
    - Supply-chain compromise

2024 Statistics – Cost of a Data Breach

- Global average total cost = **$4.88 million**
- U.S. average total cost = **$9.36 million**
- Healthcare sector highest = **$11.45 million per incident**
- Average time to identify + contain = **295 days**

VORYS

Global Connectivity = Global Vulnerability

- **5.5** billion active internet users worldwide
- **85%** of organizations store sensitive date in the cloud
- **70%** of breaches involve third-part or vendor systems
- **68%** of employees use personal devices for work

VORYS

What's Changed Since 2024

- **Mega-breaches defined 2024:** Ticketmaster (560 M records), Change Healthcare (190 M), AT&T (110 M)
- **AI-driven scams surge:** deepfake voices & video used in wire-fraud and HR-payroll attacks
- **Text-based phishing ("smishing") up over 60 % YoY:** now the most common mobile fraud vector
- **State privacy expansion:** Texas TDPSA (July 2024), Oregon Privacy Act (July 2025), Delaware and Montana laws active

Development of a Modern Data Privacy Strategy

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP

513.723.4000| ewrichardson@vorys.com | bdcraft@vorys.com

VORYS

Develop a Modern Data Privacy Strategy

- *Not a static checklist — a living process that evolves with technology*
- Focus on detection + response, not just protection
- Integrate mobile and text-based threat awareness into training (smishing, MFA fatigue)

Develop a Modern Data Privacy Strategy

- Include a human-impact lens; assess how quickly personal information can be weaponized if leaked
- **Involve counsel early:** legal, PR, and compliance must coordinate within 24 hours of detection
  - Involve counsel in the investigation from the beginning of an investigation, in order to assert as broadly as possible work product and attorney-client privilege over the aspects of a data breach response.

Develop a Modern Data Privacy Strategy
(cont'd)

- Maintain an accurate data inventory across all platforms (servers, mobile, cloud, third-party)
- **Retain PII no longer than necessary**
  - Apply the "Data Diet" principle: keep only what's essential for business operations
  - Implement data minimization and deletion schedules

Develop a Modern Data Privacy Strategy
(cont'd)

- **Retain PII no longer than necessary (cont'd)**
  - Keep PII only as long as necessary for your business purposes.
    - Depends on business needs and practicalities, but periodic efforts should be made to review and purge data that is no longer necessary (i.e., PII of departed and/or terminated employees; expired customer accounts).

Develop a Modern Data Privacy Strategy
(cont'd)

- Map where personal data intersects with mobile communication — texts, messaging apps, and employee devices

- For counsel: limiting stored data narrows breach scope → smaller regulatory and personal impact exposure

Develop a Modern Data Privacy Strategy
(cont'd)

- **More than a technical problem**
  - A data breach isn't just an IT issue — it's a human event
  - Private details like health, finances, or family data can be exposed
  - The result is fear, embarrassment, and loss of control
  - Every breach affects real people, not just data records

Develop a Modern Data Privacy Strategy
(cont'd)

- **Practical and Financial Consequences**
  - Identity theft and financial fraud may follow a breach
  - Damaged credit can affect housing, employment, and loans
  - Victims spend months or years repairing their records
  - Stress and time loss carry their own financial cost

Develop a Modern Data Privacy Strategy
(cont'd)

- **Real-World Examples of Personal Consequences**
  - Change Healthcare Breach (2024): Exposed protected health information (PHI) of millions, risking identity theft and medical fraud.
  - Ticketmaster Breach (2024): 560M users affected; personal data sold on dark web.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Real-World Examples of Personal Consequences (cont'd)**
  - AT&T Breach (2024): 110M records leaked, leading to SIM-swapping and phishing.
- Each breach increases risk of fraudulent accounts, social engineering, and emotional distress.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Responding to Data Theft: Protecting Yourself**
  - Act quickly: change passwords, enable multi-factor authentication (MFA).
  - Freeze or monitor credit through major bureaus.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Responding to Data Theft: Protecting Yourself (cont'd)**
  - Watch for follow-on scams: fake refund or identity verification requests.
  - Report fraudulent use to the FTC, credit agencies, and local law enforcement.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Evolving Text-Based Phishing ("Smishing") Threats**
  - Smishing = phishing via SMS or messaging apps.
  - Attacks rose over 60 % in 2024 – now the most common mobile fraud vector.
  - Texts often impersonate banks, delivery services, or HR departments.
  - AI tools create realistic spoof messages and deepfake voices.
  - Goal: harvest credentials, install malware, or trigger payments.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Recognizing and Avoiding Smishing Attempts**
  - Red flags: Urgent language, spelling errors, odd links, unfamiliar numbers.
  - Never click links or download attachments from unsolicited texts.
  - Verify the sender using official contact channels or apps.
  - Enable spam filtering and report scam texts to 7726 ("SPAM").
  - Train employees to pause and confirm before responding to any unexpected text.

Develop a Modern Data Privacy Strategy
(cont'd)

- **When a Suspicious Text Becomes a Privacy Threat**
  - Phishing texts don't just target passwords — they target people.
  - Attackers now use stolen data to personalize scams and harass victims directly.
  - A fake delivery message can turn into identity theft, fraudulent charges, or reputational harm.

Develop a Modern Data Privacy Strategy
(cont'd)

- **When a Suspicious Text Becomes a Privacy Threat (cont'd)**
  - Once personal data is misused, the incident crosses from cybersecurity to data privacy and personal safety.
  - Knowing when to escalate a text message from "annoyance" to "reportable incident" is critical.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Due Diligence and Oversight: What to Require Up Front**
  - Request SOC 2 Type II reports and certifications annually.
  - Verify cyber and social-engineering insurance coverage; ask for endorsements covering text-message and impersonation fraud.
  - Require vendors to flow down identical protections to all subcontractors.

Develop a Modern Data Privacy Strategy
(cont'd)

- **Due Diligence and Oversight: What to Require Up Front (cont'd)**
  - Review incident-response playbooks during onboarding, not after an event.
  - For legal departments: maintain a vendor-risk inventory reviewed quarterly by counsel.

Develop a Modern Data Privacy Strategy

(cont'd)

- **Responding to Text-Based Fraud and Harassing Messages**
  - Do not reply or engage — even "STOP" can confirm your number is active.
  - Document messages: take screenshots, save numbers, note dates/times.
  - Report immediately to the FTC and FCC; contact law enforcement if threats are made.

Develop a Modern Data Privacy Strategy

(cont'd)

- **Responding to Text-Based Fraud and Harassing Messages**
  - Block senders and use phone security features to filter future texts.
  - Employers: establish internal reporting channels for harassing or fraudulent communications.

Data Security Best Practices

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP

513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS

Data Security Best Practices

- **Data Security Best Practices: Protecting Both People and Data**
  - Identify all personally identifiable information (PII) and sensitive business data you hold.
  - Map where that information resides — servers, laptops, mobile devices, texts, and cloud platforms.
  - Determine which state and federal laws apply to each category of data.
  - Understand how a breach would affect *individuals* (identity theft, stalking, harassment) as well as the organization.

Data Security Best Practices

- **Build and Rehearse an Incident Response Plan (IRP)**
  - Include smishing, AI-based impersonation, and harassment reports as incident types.
  - Designate counsel as the incident-response lead to ensure privilege and ethical compliance.
  - Establish clear communication channels — phone, text, Teams — and know who can use them if systems go down.
  - Document notification procedures for individuals and regulators.

Data Security Best Practices

- **Practice Makes Prepared: Tabletop Exercises & Expert Support**
  - Simulate text-based phishing and social-engineering events.
  - Practice decision-making under time pressure — when to involve regulators, when to notify individuals.
  - Retain a forensic investigator and PR firm before a breach occurs.
  - Ensure exercises include mock consumer harassment or fraud scenarios (e.g., follow-on scams after a breach).
  - Evaluate post-exercise reports for gaps in ethics, communication, or privilege.

Data Security Best Practices

- **Use clear and consistent language in your data security policies**
  - Conflicting and vague policy language creates uncertainty as to cybersecurity requirements and breach response measures.
  - Incorporate relevant aspects of recognized cybersecurity frameworks into policies and procedures (e.g., NIST, FedRAMP, ISO).
  - Adherence to recognized cybersecurity frameworks can provide an affirmative defense to data breach litigation under O.R.C. § 1354.

Data Security Best Practices

- **Technical Hygiene Still Counts**
  - Regularly install firmware updates and MFA upgrades.
  - Segment networks to contain breaches.
  - Encrypt sensitive and personal data — including data on phones and text-messaging platforms.
  - Require multi-factor authentication and time-based access expiration.
  - **Document these controls**: Regulators increasingly view them as *minimum* standards of care.

Data Security Best Practices

- **Regularly change passwords**
  - Requiring your employees to regularly change their passwords keeps access credentials from becoming stale and creates “moving targets” that are more difficult for hackers to hit.
  - Requiring multi-factor authentication (“MFA”) for remote and other access to systems and networks is also highly recommended.

Data Security Best Practices

- **Insulate sensitive data and network locations from public access points**
  - Have measures in place to ensure that guest Wi-Fi and public terminals cannot serve as backdoors into your company's network or databases.
- **Suspend inactive accounts after termination or lack of use**
  - Periodic removal of unused accounts eliminates a potential blind spot in your system's security.

Data Security Best Practices

- **Establish procedures for the preservation of data when a breach occurs**
  - Resist the urge to format servers following a malware infection, so as to preserve important data regarding the extent of infection and possible exfiltration of data.
- **Require vendors to indemnify against breaches and other cyberliability**
  - Include provisions in your company's vendor agreements that provide for indemnification if the vendor is the source of a breach of your data.

Data Security Best Practices

- **Carry appropriate cyberliability insurance**
  - Insurers offer broad ranges of cyberliability insurance policies that cover many of the cybersecurity risks that businesses and entities of all types and sizes face.

State Notification and Data Privacy Laws

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP

513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS

Notification Laws

- **State Breach Notification Landscape (2025 Update)**
  - All 50 states, D.C., Puerto Rico, Guam, and the U.S. Virgin Islands now have active breach-notification statutes.
  - 2024–25 trend: shorter notice windows (30–45 days) and expanded definitions of "personal information."
  - New state privacy acts (TX, OR, MT, DE) include explicit consumer-notice and data-handling duties.
  - Several states now require notice of harassing or fraudulent use of personal data (e.g., cyberstalking, impersonation).
  - Counsel must verify which resident's law applies —not just where the breach occurred.

Notification Laws

- **Notification laws typically consist of:**
  - Definitions
    - “Breach” and “PII” definitions are very important, as these typically trigger requirements
  - Safe harbor
  - Notification requirements (timing, method)
  - Whether notification should be made to law enforcement, state AG, regulators
  - Enforcement/penalty provisions

Ohio's Notification Law

O.R.C § 1349.19(A)(6), (A)(7)

- **Person**
  - [A]n individual, corporation, business trust, estate, trust, partnership, association, sole proprietorship, financial institution or other business entity if it conducts business in this state
- **Personal Information**
  - An individual's first and last name or first initial and last name in combination with any one (1) or more of the following data elements:
    - Social security number
    - Driver's license number or state ID card number
    - Account number or credit or debit card number, in conjunction with any required security code, access code, or password

Ohio's Notification Law

O.R.C § 1349.19(A)(7)(b)

- Personal information **does not** include **publicly available information** that is lawfully made available to the general public from **federal, state or local government records** or distribution through **bona fide news media**
  - Newspapers, magazines, radio, television
  - Publications of charitable/nonprofit corporations or associations

Ohio's Notification Law

O.R.C § 1349.19(A)(1)(a)

- **"Breach of the security of the system"**
  - **Unauthorized** access
  - **Computerized** data
  - Compromises the security or confidentiality of **personal information** owned or licensed by a **person**
  - Causes, reasonably is believed to have caused, or reasonably is believed will cause a **material risk of identity theft or fraud** to the person or property of a **resident of this state**

Ohio's Notification Law

O.R.C § 1349.19(B)

- When must a disclosure be made?
  - Owner or licensee of computerized data containing **personal information** shall disclose any **breach of the security system** following discovery or notification of the breach to **any resident** whose data was, or reasonably believed to have been, **accessed and acquired by an unauthorized person** if the breach causes or reasonably is believed will cause a **material risk of identity theft or fraud**
- Time for disclosure:
  - Disclosure must be made in the **most expedient time possible** but **not later than 45 days** following discovery of the breach

Ohio's Notification Law

O.R.C § 1349.191(E)

- Notification may be provided through:
  - Written notice;
  - Electronic notice (if primary communication with resident to whom disclosure must be made is by electronic means);
  - Telephone notice;
  - Substitute notice, if information holder demonstrates cost of notice exceeds $250,000 or class of affected persons exceeds 500,000
    - Email notice
    - Conspicuous posting of notice on business entity's website
    - Notification to major media outlets (if audience exceeds 75% of the population of the state)

Ohio's Notification Law

O.R.C § 1349.191(E)(5)

- Substitute notice for business entities with ten (10) employees or fewer and cost of providing notice exceeds $10,000
  - Newspaper notice:
    - Circulation in the geographic area in which the business is located
    - Paid advertisement covers at least one-quarter of a page
    - Published in the newspaper at least once a week for three consecutive weeks
  - Conspicuous notice on business entity's website
  - Notification to major media outlets in the geographic area in which the business is located

Ohio's Notification Law

O.R.C § 1349.191(C), (G)

- Permissible Delay:
  - Notification may be delayed if law enforcement agency determines notification will **impede criminal investigation**
- If circumstances require notification of more than 1,000 persons at one time:
  - Entity must also notify all consumer reporting agencies and credit bureaus

Ohio's Notification Law

O.R.C § 1349.191(F)

- **Exemptions:**
  - Financial institutions, trust companies, or credit unions that are required by federal law to notify customers of an information security breach and are subject to examination by a regulatory agency for compliance with the applicable law (e.g., Gramm-Leach-Bliley Act (15 U.S.C. § 6801, *et seq.*); Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (12 C.F.R. Parts 30, 364, 568))
  - A covered entity as defined in 45 C.F.R. Part 160.103 (definition section of HHS Standards for Privacy of Individually Identifiable Health Information)
    - Includes health plan, health care clearinghouse, health care provider who transmits health information in electronic form

Ohio's Notification Law

O.R.C § 1349.191(H), (I)

- Ohio's Notification Law includes no provisions creating a private right of action for a violation
- Any waiver of the law's requirements is contrary to public policy and void/unenforceable
- **Enforcement**:
  - Ohio AG may conduct an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of the law

Massachusetts Notification Law

- Amendments to Massachusetts Notification Law:
  - Expansion of information that must be reported
  - Imposition of new requirements on compromised entities
  - Additional clarification as to when entities are required to issue notice of a breach
- Changes took effect on April 11, 2019
- Represents trend toward more stringent notice requirements

Massachusetts Notification Law

- Additional Requirements:
  - Entities that have experienced a data breach involving the personal information of Massachusetts residents must inform the Massachusetts AG and Office of Consumer Affairs and Business Regulation “whether the person or agency maintains a written information security program” (WISP).
  - New requirement provides regulators with mechanism to penalize entities who have failed to implement a compliant WISP.

Massachusetts Notification Law

- Additional Requirements:
  - General requirement of 18 months of credit monitoring services must be provided when Social Security numbers are compromised
  - Breached credit reporting agencies must provide 42 months of free credit monitoring services when Social Security numbers are involved
  - Affected individuals cannot be required to waive their right to a private right of action as a condition to receive the credit monitoring services

Massachusetts Notification Law

- Additional Requirements:
  - Companies must disclose to Massachusetts regulators the types of personal information compromised in the breach
  - Companies must inform affected residents that they have the right to place a security freeze on their credit reports at no charge
  - If a subsidiary is breached, the notification to affected residents must include the name of the parent or affiliated corporations

Massachusetts Notification Law

- Additional Requirements:
  - Notice cannot be delayed on grounds that the total number of residents affected by the breach is not yet known
  - Companies must give notice “as soon as practicable and without unreasonable delay” once an entity “knows or has reason to know” of a breach of a resident’s personal information

California Privacy Law
CCPA / CPRA / CPPA Regulations

- Comprehensive law regulating how businesses collect, use, and share personal information of California residents
- Originally enacted June 28, 2018; amended by the California Privacy Rights Act (CPRA), effective January 1, 2023
- California Privacy Protection Agency (CPPA) now oversees enforcement and rulemaking
- Final CPPA regulations (July 24, 2025) require risk assessments, cybersecurity audits, and limits on automated decision-making
- California Delete Act (SB 362) (effective January 1, 2026) will create a single opt-out portal for all registered data brokers

CA Consumer Privacy Act ("CCPA")

- Broadly applies to "businesses"—any for profit legal entity (e.g., corporation, partnership, LLC) that does business in the State of California, that collects consumers' personal information, and that meets one of the following thresholds:
  - Has gross revenue in excess of $25,000,000;
  - Buys, receives, or sells for commercial purposes the personal information of 50,000 or more consumers, households, or devices; **or**
  - Derives 50 percent or more of its revenue from selling consumers' personal information

CA Consumer Privacy Act ("CCPA")

- Law creates new privacy rights for consumers:
  - The right for consumers to know what personal information is being collected
  - The right to know whether the personal information is being sold or disclosed
  - The right to prevent the sale of one's personal information
  - The right to access one's personal information; and
  - The right to enjoy equal service and price even if one exercises his or her privacy rights.

CA Consumer Privacy Act ("CCPA")

- Under the law, businesses must inform consumers of categories of information being collected and the purposes for which the information is collected
- Consumers can request that the business disclose:

1. The categories of the consumers' personal information collected
2. The sources of the collected information
3. The business purposes for the collection or sale of the information
4. The identities of third parties with whom the information has been shared
5. The specific pieces of personal information collected.

CA Consumer Privacy Act ("CCPA")

- The law creates a private right of action for consumers' claims based on the **unauthorized access** and **exfiltration**, **theft**, or **disclosure** of **unencrypted and nonredacted** personal information.
- Allows for statutory damages that are the greater of:

  (a) between $100 and $750 per consumer per incident; or

  (b) actual damages

- Also provides for administrative enforcement with penalties up to $2,500 ($7,500 if intentional) per violation.

CA Consumer Privacy Act ("CCPA")

- **2025 Amendments: New Regulatory Focus**
  - On July 24, 2025, the CPPA approved significant amendments emphasizing:
    - Automated Decision-Making Technology (ADMT)
    - Cybersecurity Audits
    - Risk Assessments
    - Delete Request and Opt-Out Platform (DROP) regulations
  - Marked shift toward AI accountability and documented cybersecurity governance

CA Consumer Privacy Act (“CCPA”)

- **Automated Decision-Making Technology (ADMT)**
  - Applies to businesses using AI or profiling systems affecting employment, credit, insurance, or eligibility decisions
  - Requires specific notices describing logic and likely outcomes
  - Consumers gain the right to opt-out of certain automated decisions
  - Businesses must provide meaningful information about the use and impact of ADMT
  - Compliance expected to phase in by January 1, 2027

CA Consumer Privacy Act ("CCPA")

- **Risk Assessment Requirements**
  - Required for high-risk data processing (e.g., sensitive data, large-scale profiling, minors)
  - Must evaluate:
    - Purpose and proportionality of processing
    - Safeguards and mitigation steps
    - Risks to consumer privacy and security
  - Initial compliance begins January 1, 2026
  - Attestations due annually beginning April 1, 2028–2030 depending on business size

CA Consumer Privacy Act ("CCPA")

- **Cybersecurity Audits**
  - Annual independent cybersecurity audits required for higher-risk businesses
  - Must assess technical, organizational, and governance controls
  - Emphasizes continuous testing, documentation, and remediation tracking
  - Certification submissions to CPPA based on revenue tier:
    - > $100 million – April 1, 2028
    - $50–100 million – April 1, 2029
    - < $50 million – April 1, 2030

CA Consumer Privacy Act ("CCPA")

- **Delete Act (SB 362) and DROP System**
  - Establishes a centralized deletion mechanism for data brokers
  - Consumers can submit one deletion request via the CPPA's DROP portal
  - Data brokers must check the DROP system every 45 days and process valid requests
  - Effective dates:
    - January 1, 2026 – DROP portal available
    - August 1, 2026 – mandatory compliance for data brokers
  - Enhances consumer control and simplifies deletion requests across the industry

Texas (TDPSA) Overview

- Became effective July 1, 2024 (with some opt-out provisions effective Jan 1, 2025)
- Applies to entities that: (a) conduct business in Texas or produce products/services consumed by Texas residents; (b) process or sell personal data; (c) are not a “small business” as defined by SBA
- Grants Texas residents rights to: access their personal data; correct; delete; obtain portable copy; opt-out of targeted advertising, sale of personal data, profiling
- Obligations for businesses include: transparency notices, data minimization, reasonable security, special disclosures when selling sensitive or biometric data, a perpetual 30-day cure period after violation notice
- Enforcement: Exclusively by Texas Attorney General; no private right of action; penalties for non-remediated violations up to $7,500 per violation

Oregon (OCPA) Overview

- Signed into law July 18, 2023; most provisions effective July 1, 2024 (non-profits have until July 1, 2025)
- Applies to controllers/processors doing business in Oregon or providing goods/services to Oregon residents, and meeting one of: (i) process personal data of ≥ 100,000 consumers; or (ii) process ≥ 25,000 and derive ≥ 25% of revenue from sale of personal data
- Consumer rights: access, correct, delete, opt-out of sale/targeted advertising/profiling, portability; controller must respond within 45 days (plus extension)
- Business obligations: privacy notices, data-protection assessments for high-risk processing (sale, profiling, sensitive data), vendor/processor contracts, limitation of collection to “adequate, relevant and reasonably necessary”
- Enforcement: Only state AG; no private right of action; cure period required before action; non-profits covered after 2025

Legal Ethics in Data Privacy Matters

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP

513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS
New thinking.
Since 1909.

Legal Ethics in Data Privacy Matters

- Data privacy now intersects with every aspect of client representation
- New threats include AI-driven impersonation, smishing, and targeted harassment
- Lawyers must adapt traditional duties to digital communication and data-handling risks
- Ethical rules emphasize:
  - Competence – staying current on privacy laws and technology
  - Confidentiality – safeguarding client data and communications
  - Diligence – responding quickly to breaches or fraudulent activity
  - Communication – keeping clients informed after incidents

Law Firms and Legal Departments

- Law firms are ethically required to ensure that their attorneys are observing and complying with these ethical requirements.
  - Rule 5.1(a)
    - A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

Law Firms and Legal Departments

- Rule 5.1 – Relevant Commentary
  - (2) Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct. Such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.

Law Firms and Legal Departments

- Data Privacy Risks for Law Firms and Legal Department
  - Law firms and legal departments manage large volumes of personal and confidential client data
  - Threats now extend beyond hacking to include privacy misuse and data exposure
  - Common privacy risks include:
    - Inadvertent disclosure of client information via email, text, or cloud sharing
    - Unauthorized use or retention of client or employee personal data
    - Improper AI tool use that uploads confidential information to third-party servers
    - Harassing or fraudulent communications targeting clients or staff using leaked data
    - Third-party vendor leaks involving document-hosting or e-discovery platforms
  - Privacy compliance now requires monitoring, training, and documented safeguards

Law Firms and Legal Departments

- **The Human Element in Data Privacy**
  - Most privacy failures occur through everyday actions, not sophisticated attacks
  - Examples of human-driven breaches:
    - Forwarding client materials to personal or group chats
    - Uploading confidential drafts to AI or translation tools
    - Auto-syncing case files to personal cloud storage
    - Over-sharing sensitive details in marketing or client updates
  - Each error can trigger privacy-law violations and ethical duties to disclose
  - Mitigation requires:
    - Access controls and data-loss prevention tools
    - Clear firm policies on AI use and remote work

ABA Formal Opinion 483: Overview

- Issued in 2018
- Addresses how lawyers must respond ethically when client data is compromised.
- Clarifies duties under Model Rules 1.1 (Competence) and 1.6 (Confidentiality).
- Emphasizes preparedness, reasonable security, and timely response as ethical requirements — not optional best practices.
- Notes that a breach does not automatically equal misconduct if the lawyer took reasonable preventive and remedial measures.

Duties After a Breach (Per Formal Opinion 483)

- **Act promptly** to investigate and mitigate the incident.
- **Determine scope and impact —** what information was accessed and which clients are affected.
- **Notify current clients** if material client information was or is reasonably suspected to be compromised.
- **Maintain transparency**: disclose enough facts for clients to make informed decisions about representation.
- **Implement corrective measures** to strengthen systems and prevent recurrence.
- **Document response** efforts to show compliance with ethical obligations.

Ethics Rules: Competence

- **Rule 1.1 - Competence**
  - A lawyer shall provide competent representation to a client.
  - Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.
  - Comment (6): To maintain competence, lawyers must stay abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.
  - Today, competence includes understanding:
    - Data-privacy and breach-notification laws
    - Risks of using AI and cloud-based tools in client work
    - Information-governance and retention policies affecting client data

Ethics Rules: Competence

- **Competence and Data Privacy**
  - Data-privacy and information-security issues can impact any client, in any industry.
  - Lawyers must have enough knowledge of:
    - Privacy statutes and breach-response frameworks to advise clients effectively
    - AI data-use practices to avoid inadvertent disclosure of confidential information
    - Third-party vendor policies and data-transfer safeguards
  - Competence also means knowing when to bring in technical experts and ensuring clients receive accurate, compliant guidance.

Ethics Rules: Diligence

- **Rule 1.3 – Diligence**
  - A lawyer shall act with reasonable diligence and promptness in representing a client.
  - Comment (3): Procrastination undermines trust and can harm the client's interests. In privacy matters, diligence requires:
    - Prompt action when personal data is compromised or misused
    - Coordinating with clients and vendors on timely notification and remediation
    - Ensuring privacy and data-handling policies are reviewed and updated regularly

Ethics Rules: Diligence

- **Diligence and Data Breaches**
  - Whenever a data breach occurs, time is of the essence
  - Unreasonable delay in assessing and responding to a data breach can irreparably damage a client's business and ability to defend in resulting litigation
  - Notifications laws require an entity that has experienced a data breach to move quickly
    - In some cases a breached entity must provide notices within 72 hours (*See* 23 NYCRR 500)

Ethics Rules: Communication

- **Rule 1.4 – Communication**
  - Lawyers must keep clients reasonably informed and explain matters as necessary for informed decision-making.
  - Effective communication in data-privacy incidents means:
    - Providing timely updates after a breach or data-exposure event
    - Translating complex privacy and regulatory issues into plain language
    - Advising clients on the implications of disclosing or withholding information
    - Using secure communication channels to preserve confidentiality

Ethics Rules: Communication

- **Communication in Privacy Contexts**
  - Lawyers should be familiar with data-privacy frameworks to explain client obligations clearly.
  - Strong communication includes:
    - Identifying privacy risks early in representation
    - Explaining regulatory timelines for notice and cooperation
    - Maintaining transparency about firm and vendor data-protection measures
  - Proactive communication strengthens trust and compliance culture.

Ethics Rules: Confidentiality

- **Rule 1.6 – Confidentiality of Information**
  - Lawyers must not reveal information related to the representation of a client without consent.
  - Confidentiality now includes safeguarding digital and personal information from exposure or misuse.
  - Reasonable precautions depend on:
    - Sensitivity of information (e.g., health, financial, or identifying data)
    - Privacy laws governing the data
    - Security of the communication method used to transmit it

Ethics Rules: Confidentiality

- **Rule 1.6 – Confidentiality of Information (Relevant Commentary, cont'd)**
  - (15) When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may 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. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

Ethics Rules: Safekeeping Property

- **Rule 1.15 – Safekeeping Property**
  - (a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client, third person, or both in the event of a claim by each to the property. The separate account referred to in the preceding sentence shall be maintained in a bank which has agreed to notify the Kentucky Bar Association in the event that any overdraft occurs in the account. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of five years after termination of the representation.

Ethics Rules: Confidentiality and Safekeeping Property

- **Confidentiality**
  - Lawyers and law firms are prime targets for cybercriminals due to the types of documents and information with which they are entrusted
  - Potential Targets:
    - Privileged and confidential documents
    - Financial records
    - Trust Account

Ethics Rules: Confidentiality and Safekeeping Property

- A lawyer's / law firm's / legal department's adoption of appropriate and reasonable cybersecurity measures and protections fall within the scope of the Confidentiality and Safekeeping Property Rules
- Such steps are required by the lawyer's duty to take "reasonable precautions to prevent the information from coming into the hands of unintended recipients" and to ensure that client property is "appropriately safeguarded"

Questions?

Eric Richardson
513.723.4019
ewrichardson@vorys.com

Brent Craft
513.723.4072
bdcraft@vorys.com

VORYS