Data Privacy and Cybersecurity: What Every Lawyer Needs to Know

Caution: *This material does not establish an attorney's standard of due care for a particular situation and/or in any particular community. Rather, it is our intent to encourage our audience to act in a manner which may be well above the standard of due care in order to attempt to avoid claims having merit, as well as those without merit. This material does not contain legal advice and is for general educational purposes only. The views expressed herein are those of the presenters and are not necessarily those of Lewis Brisbois.*

Simone McCormick

- Partner at Lewis Brisbois Bisgaard & Smith LLP in Portland, Oregon;
- Member of Lewis Brisbois' national Data Privacy and Cybersecurity Team;
- Represents clients in privacy and employment matters in state and federal courts, administrative hearings and in government investigations;
- Acts as breach coach in data incidents, conducts risk analysis, audits, trainings and investigations;
- Prepares contracts (e.g. BAAs), specifically tailored policies, procedures and handbooks;
- Counsels clients in compliance, risk management and best practices;
- Is a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP).

Bryan Thompson

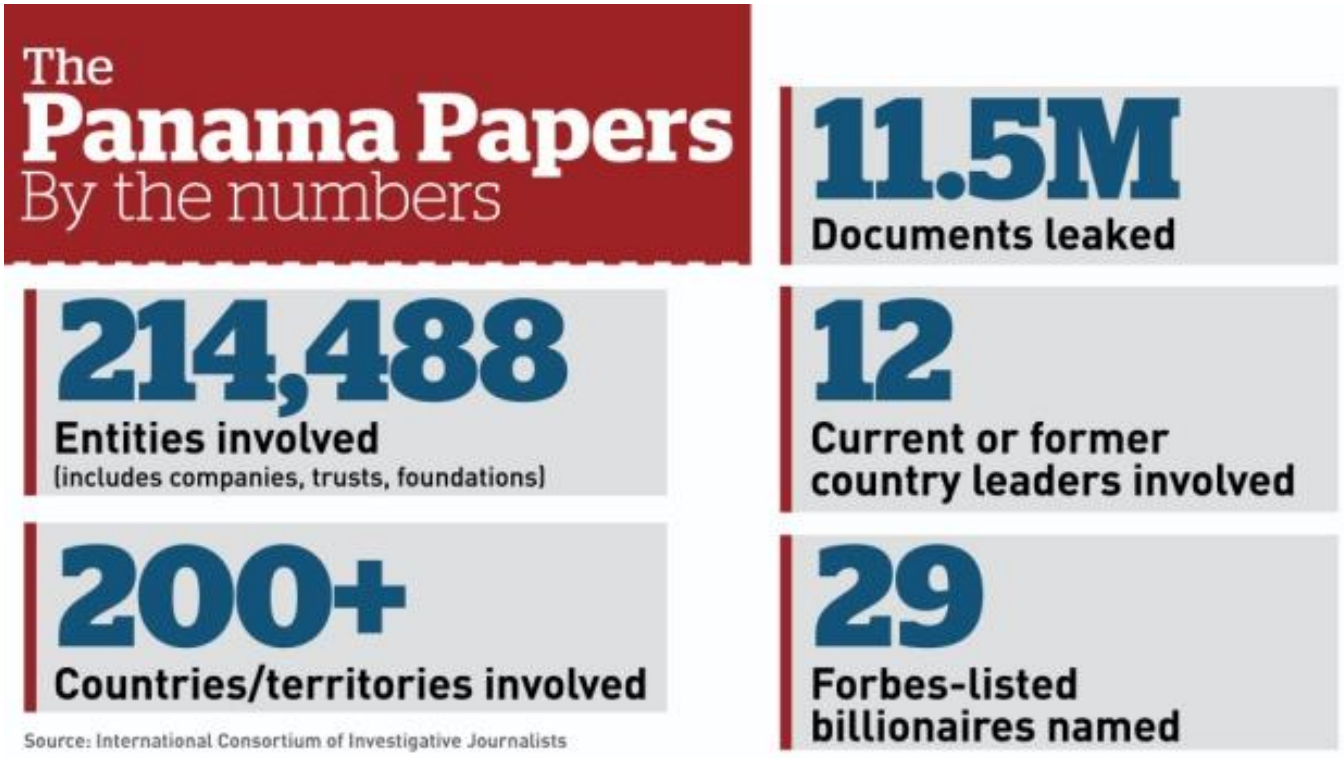
- Associate at Lewis Brisbois Bisgaard & Smith LLP in Portland, Oregon;
- Member of Lewis Brisbois' Data Privacy & Cybersecurity Team;
- Assists clients in data security incident response, including regulatory inquiries;
- Assists with privacy and security compliance by drafting privacy and security policies and facilitating security audits;
- Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP);
- Captain in the U.S. Army Reserve, Judge Advocate General's (JAG) Corps

Law Firm Threats of the 21st Century

Threats

"…There are only two types of companies: those that have been hacked and those that will be."

Robert Mueller, 2012


The
Panama Papers
By the numbers
11.5M
Documents leaked
214,488
Entities involved
(includes companies, trusts, foundations)
12
Current or former
country leaders involved
200+
Countries/territories involved
29
Forbes-listed
billionaires named
Source: International Consortium of Investigative Journalists

Five Common Scenarios

1. Ransomware Attack
2. Microsoft 365 Email Compromise
3. Misdirected Email
4. Stolen Device (containing confidential files)
5. …

5. Improper Disposal

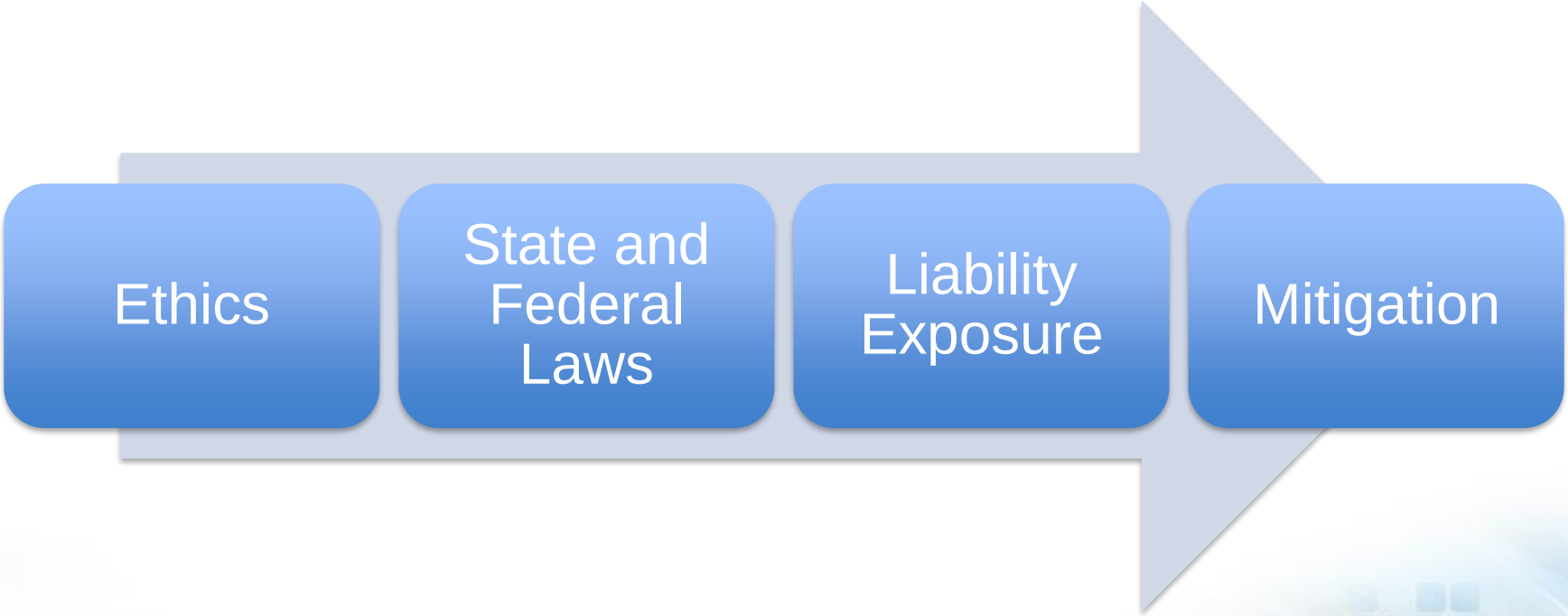
Types of Protected Data

- HR Files
  - Personal Information (clients, employees, 3Ps)
  - Protected Health Information (PHI)
- Law Firm Internal Documents
  - Financial Information
- Legal Files
  - Confidential client information, Work Product (Analysis & Strategies)
  - Tax Returns, financial information, SSN, PII, PHI
  - Trade secrets, IP

Why Are Law Firms Targets?

- Money (extortion, payment credentials)
- Data with direct black market value (PHI, SSN, PII)
- IP/Trade secrets
- Strategic Information (litigation and transactions)
- Whistleblower
- Public exposure
- Retribution/harm

Roadmap


Ethics
State and Federal Laws
Liability Exposure
Mitigation

Ethical/Professional Responsibilities

Protecting Client Communications and Secrets

Duty of Confidentiality

- Lawyers have the duty to keep inviolate client confidences/secrets.
  - Exceptions:
    - (permissive/mandatory) to prevent a criminal act likely to result in substantial bodily harm
    - Informed client consent
- Source:
  - Oregon Rules of Professional Conduct 1.6/ABA Model Rule 1.6
  - Evidence Codes – attorney-client privilege

Duty of Competence

- Lawyers have to perform their legal services competently and diligently
- They are prohibited to commit intentional, reckless or negligent failures in carrying out the legal services.
- This includes the supervision of reports, vendors and staff.
- Source:
  - Oregon Rules of Professional Conduct 1.1, 1.3/ABA Model Rule 1.1
  - Common Law – Negligence/Malpractice

Duty of Communicate

- Lawyers have to promptly inform clients
  - Significant developments in case/representation;
  - Adverse risks or outcome potentials
- Source:
  - Oregon Rules of Professional Conduct1.4 /ABA Model Rule 1.4
  - Common Law – Negligence/Malpractice

Putting It All Together

- **A lawyer must act *competently* to preserve *confidential* client information.**
  - The lawyer should keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology (ABA Model Rules, R. 1.1 Comment [8])
  - It requires the lawyer to act competently to safeguard information relevant to the representation of a client against unauthorized disclosure by the lawyer or persons under his/her supervision (ABA Model Rules, R. 1.6 Comment [18])

BUT Safe Harbor: unauthorized access is NOT a violation if the lawyers makes reasonable efforts

ABA Model Rules

- **Reasonable Efforts to Prevent Unauthorized Disclosure**
  - Attorneys have the obligation to… “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” (ABA Model Rules 1.6 [Comment 18]) Reasonable efforts depends on:
    - The sensitivity of the information
    - The likelihood of disclosure if additional safeguards are not employed
    - The costs of employing additional safeguards
    - The difficulty of implementing the safeguards,
    - The extent to which the safeguards adversely affect the lawyer’s ability to represent clients

ABA Formal Opinion 477 (May 2017)

- Reasonable Efforts to Prevent Unauthorized Disclosure Guidelines
  1. Understand the Nature of the Threat
  2. Understand How the client Confidential Information is Transmitted and where it is Stored
  3. Understand and Use Reasonable Electronic Security Measures
  4. Determine How Electronic Communications About Clients Matters Should be Protected
  5. Label Client Confidential Information
  6. Train Lawyers and nonlawyers Assistants in technology and Information Security
  7. Conduct Due Diligence on Vendors

ABA Model Rules

- **Advise Clients About Potential Disclosure/Communicate Risks**
  - Lawyers have to advise clients about risks associated with email communications that may potentially compromise the client confidentiality depending on the server, device and transmission mode. (ABA Standing Comm. on Ethics and Prof. Resp., 11-459 Formal Opinion 2011.)
- When a lawyers reasonably believes that highly sensitive/confidential client information is being transmitted so that extra measures to protect the email are warranted, the lawyer should inform the client about the risks involved. (ABA Model Rules 1.4 (a)(1)&(4))
- The client may insist or require the lawyer to undertake or conduct certain forms of communication (ABA Model Rules 1.6 Comment [18])

ABA Model Rules

- **Encrypt emails**?
  - Use of *un*encrypted email generally remains acceptable if the lawyer has undertaken *reasonable efforts* to prevent inadvertent + unauth. access to client information
  - **BUT** a lawyer may be required to take special security precautions to protect against the inadvertent + unauth. Disclosure when required by agreement or by law.
  - (ABA Formal Opinion 477 (May 2017);
  - See also/Compare with: (New Jersey Opinion 701 (2006), California Formal Opinion No 2010-179, Pennsylvania Formal Opinion 2011-200 Texas Opinion No. 648 (Apr 2015)

Keep Abreast of Technological Changes

- Attorneys have to “keep abreast of changes in the law practice, including the benefits and risks association with relevant technology.” (Comment [8] to Model Rules 1.1.)
- Network Administration-Outsourcing
- OK to utilize off-site network administrators to assist in the operation of the law practice. (Ill. State Bar Ass., Adv. Opinion 10-01, 2010)

Vendor Vetting

- Carefully select the vendor, incl. cloud software and hosting services providers,
- Validate credentials: reputable company, established policies/protocols/systems,
- Evaluate vendors' policies and procedures and security systems - they at a minimum must match the lawyer's obligations,
- Address data transmission- and sub-vendor issues,
- Ensure enforceability of obligation to preserve client confidentiality/security. (ABA Formal Opinions Nos. 08-451, 95-398; Oregon State Bar Ethics Opinion 2011-188, New York State Bar Association Opinion 842, Pennsylvania Bar Association Formal Opinions 2010-200 and 2011-200, California State Bar Formal Opinions Nos. 2010-179, 2012-184)
- See: https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

State Bar Opinions

- Security Assessment Based on Circumstances
  - Act competently means to “safeguard information relating to the representation of a client against unauthorized disclosure.” Factors: assessment of technology, security, degree of sensitivity, impact on disclosure and legal ramifications. (Cal. State Bar Standing Comm. on Prof. Resp. and Conduct, Formal Opinion No. 2010-179.)
- Avoid Free Wi-Fi
  - Absent security measures, avoid using the public wireless connection or notify the Client of possible risks …and seek informed consent. (Cal. State Bar Standing Comm. on Prof. Resp. and Conduct, Formal Opinion No. 2010-179.)

State Bar Opinions

- Electronic Storage
  - Reasonable online security measures pursuant to a computer security consultant that in light of the rapid changes need periodic review. Minimally required measures include: firewalls, password protection, encryption and anti-virus measures. (State Bar of Arizona Opinion, No 05-04, 2005)
- Protect Metadata
  - Exercise reasonable care to prevent the disclosure of confidences and secrets contained in transmitted metadata (New York State Bar Association Committee of Prof Ethics, Opinion 782, 2004, Oregon State Bar Ethics Opinion 2011-187)

State and Federal Legal Requirements

Protecting Specific Types of Data

U.S. Sectoral Model to Data Protection

- Patch-work of different data protections for specific data types (sectors), both federal and in 50 states
- Principles: Privacy, Notice, Security and Notification
- Differences: Types of data, scope of protection, notice & notification requirements, enforcement power/private right of action

Federal Privacy Laws

- “Right to be left alone” & “Reasonable Expectation of Privacy” (derived from U.S. Constitution 1st, 4th and 14th Amendments)
- HIPAA
- GLBA
- FTC, Art. 5
- …

State Privacy Statutes

- Define personal information (PI)
- Protect PI
- May require breach notification to impacted individuals and AGs
- May include (specific or general) security requirements
- May provide private right of action
- Specify damages: compensatory and nominal damages awards, credit monitoring

Other Applicable State Law

- Unfair business practices statutes (OR: UTPA)
- Contract law
- Negligence
- Malpractice

Potential Liability Exposure

- Forensic Investigation/Network Remediation/Business Interruption
  - May require: Notification/Call Centers/credit monitoring
- Reputational Harm
- Financial Harm

Post Incident Government Investigations

- State Attorney General investigations
- Office of Civil Rights – HIPAA Compliance
- Federal Trade Commission – FTC Act
- State Bar Associations
  - ➔➔Penalties, CAP, disciplinary actions

Private Lawsuits

- Types of Claims:
  - Negligence
  - Breach of contract
  - Unfair trade practices
  - Breach of privacy policies
  - Statutory violations
  - Legal malpractice
- Hurdles:
  - Standing to sue/no private right of action
  - Causation of actual injury or harm

Mitigating Privacy and Security Risks

Firm Management

- Identify the firm’s digital/other data assets
- Identify potential outside risks
- Understand legal and ethical responsibilities
- Analyze security infrastructure
- Conduct a risk assessment and gap analysis
- Analyze the potential exposure
- Appoint a privacy/security team
- Appoint a privacy/security officer or administrator

Employee Training

- Training is critical for security and to mitigate risks
  - Privacy and data security policies and procedures
  - Handling and reporting data security incidents
  - Ongoing program – webinars, bulletins, awareness posters

Incident Response Planning

- Build a strong incident response team (Management, IT Security, Legal/Privacy, HR, PR/Communications, Support)
- Create an incident response plan
- Test and improve your plan
- Establish relationships with law enforcement, regulators and external resources
- Consider cyber insurance to mitigate financial risks

Security – Best Practices

- Assess the firm's system adequacy to meet the identified risks
- Exercise appropriate governance over the firm's digital assets (and third parties who store/have access)
- Continual risk assessments/pen/social engineering tests and review of external threats/risks.

Best Practices

- Computer Protection
  - Strong Password protection, changed regularly
  - Automatic lockout after reasonable time of inactivity
  - Deactivation of USB drives, if appropriate
- Encryption
  - All laptops, phones AND DESKTOPS
  - Specific stored client data encrypted (“at rest”)
  - Encryption of communications (“in transit”)
  - Specific files encrypted when sent to client (“transit AND rest”)

Best Practices

- Data Access
  - Not all data is equally sensitive
  - Restrict access to sensitive data
  - Safe remote access (VPN)
- Safe Data Transmission
  - Third-party provider with adequate security measures
  - Encrypted pdf files transmission
  - Encrypted mailed DVD
- Make Security Part of Case Intake
  - Does engagement create a privacy/security risk?
  - Has client been targeted in past by a cyber attack?

Key Takeaways

- Lawyers have ethical/professional responsibilities to protect client communications and secrets
- Any size firm can be a victim/target of data breach or cyber attack
- Firms harbor protected data
- State and federal regulations protect specific types of data, e.g. medical data or personal information
- A data breach can result in private litigation and enforcement actions
- Early detection/thoughtful incident response may limit damages
- Devise and implement an incident response plan
- Create and enforce sensible employee policies and training
- Utilize encryption, responsible data management (access, storage, use, retention), strong password protection, and ongoing risk assessments.

Questions ?

Simone McCormick
Simone.McCormick@lewisbrisbois.com
971.712.2800

Bryan Thompson
Bryan.Thompson@lewisbrisbois.com

LEWIS BRISBOIS
BISGAARD & SMITH LLP