New York State Bar Association – International Section
Seasonal Meeting Tokyo 2019

Cybersecurity Ethics and Compliance for International Law Firms and Corporate Counsel

Andre R. Jaglom, Tannenbaum Helpern Syracuse & Hirschtritt LLP, New York
Atsushi Okada, Mori, Hamada & Matsumoto, Tokyo
Diane O'Connell, PricewaterhouseCoopers LLP, New York
Jonathan Armstrong, Cordery, London
Mary Fernandez, Headrick Rizik Alvarez & Fernandez, Santo Domingo
Scott Warren, Squire, Patton & Boggs, Tokyo

November 8, 2019

1

Some 2018 Data Points On Breaches:

- 64% of respondents suffered attacks that compromised data assets, files, or IT infrastructure
- 70% could not trace origin of hacks
- 79% said hack was result of previously unknown exploit
- Antivirus products pick up only 57% of attacks
- On average, it takes 102 days to apply, test
- and fully deploy patches.

2018 Ponemon State of Endpoint Security Risk Report

2

Lawyers Are Targets

- **2012:** Wiley Rein hacked, IP and business info on solar panel manufacturer stolen by Chinese
- **2015:** Cravath, Weil Gotshal hacked
  - M&A transaction data stolen, traded on
  - Chinese hackers indicted for insider trading
- **2016:** Mossack Fonseca: Panama Papers leak of 11.5 million documents
  - Firm, clients face fines, money-laundering charges, lost political leadership positions
- **2017:** DLA Piper: One of world's largest law firms crippled for weeks by ransomware, costs in the millions
- **2018**: BC law firm victim of phishing scam
- **2019**: Jenner & Block phished for employee W-2 data

3

Lawyers Are Targets

- Last month law.com reported:

> "Based on extensive public record requests, Law.com identified more than 100 law firms that have reported data breaches to authorities across 14 states since 2014, notifying authorities that a data breach affecting the firm could have exposed individuals' personal information."

"More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse."
https://www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse/

4

Law Firms & Data Privacy Compliance
Global Law Firm Study

Good News

- 91% of law firm respondents are either very confident or somewhat confident that their Disaster Recovery plans meet their firms' needs
- 70% of firms have completed an assessment for GDPR compliance (increased from 13% in 2016) with the remaining 30% due to complete their assessment within the next six months
- 49% of firms see digital as key to delivering their firm's overall strategy, with improving client experience identified as the key area that could add the most value

5

Law Firms & Data Privacy Compliance
Global Law Firm Study

Bad News

- 73% of laws firms have suffered attacks in the last 2 years (up 28%)
- 30% have identified attacks on either a weekly or monthly basis
- 12% claim to be receive attacks on a daily basis
- 41% of attacks were based on internal individuals activity

AND

- 16% of all firms claim not to have any privacy protection framework
- 75% of those that do, test their business continuity plan annually

So, there is a disparity between the perception and the reality regarding what is necessary for the protection of information.

6

Law Firms & Data Privacy Compliance
Cloud Computing Risks

- Limited visibility:
  - what is running in the cloud,
  - what data are there,
  - who has access.
- No policies and standards => ad hoc development => gaps for intrusion
- Poor coordination between companies and vendors => loopholes and security incidents.
- Solutions:
  - Training
  - Vendor contract provisions
  - Breach response plan – IT, Legal, PR elements
  - Cyber Insurance

7

Legal Ethics and Cybersecurity in Japan

- General rules
  - Basic Act on Cybersecurity (no specific obligation)
  - APPI (security control of personal data)
- Specific rules for law firms
  - Attorney Act
    - Duty of Confidentiality: Article 23
  - JFBA Model Rules of Professional Conduct
    - Duty of Confidentiality: Articles 18 and 23
  - JFBA Information Security Guidelines
    - No legal obligation

8

New York State Bar Association
Ethics Best Practice Guidelines

- A project of the Latin American Council of the International Section, approved by NYSBA in August 2018 for voluntary adoption in jurisdictions around the world.
- **Voluntary application**. Failure to adopt these Guidelines would not be any sort of violation.
- The Guidelines consist of a set of principles, rights, duties and prohibited actions governing Lawyers and Law Firms, based on best practices in the Americas.

HEADRICK

9

New York State Bar Association
Ethics Best Practice Guidelines

- **Principle of Confidentiality**:
  - Duty to make every lawful effort to protect and hold private Confidential Information of clients.
  - Duty to make every effort to ensure that any Person she/he hires in connection with a Legal Matter and to whom the Lawyer provides client Confidential Information will defend and protect that Confidential Information.
  - In cross border matters, duty to consider and discuss differences in applicable privilege or confidentiality laws/rules with co-counsel prior to transferring information across borders.
- **Duty to properly preserve any documents delivered by the client**.
- **Prohibited Actions**:
  - Disclose the client's Confidential Information, unless authorized to do so or required to do so by a competent court;
  - Improperly withhold or fail to deliver or to safeguard any property or documentation entrusted to the Lawyer or Law Firm.

10

Law Firms & Data Privacy Compliance
DOMINICAN REPUBLIC

- **General Ethical Duty of Confidentiality**, Dominican Code of Ethics (1983)
  - "*Attorneys must preserve the secrecy of all information received from a client during its representation and after*"
  - Waiver – when completely necessary to prevent a crime or for the attorney's self-defense when prosecuted by the client.
- **Duty to Acknowledge Liability** when damages result from the attorney's negligence, inexcusable error or misconduct.

Duties on Code of Ethics are very broad and general & there is no precedent on this matter.

- **OTHER APPLICABLE/RELEVANT LAWS**:
  - Individual's right to privacy – Article 44, Dominican Constitution;
  - Privacy and Data Protection Regulation – Law 172-13;
  - Sanction for crimes and offenses committed through technology – Law 53-07.

HEADRICK

11

Legal Ethics and Cybersecurity

- Four Key Model Rules in U.S.
  - Duty of Competence: Model Rule 1.1
  - Duty of Confidentiality: Model Rule 1.6
  - Duty to Inform Client: Model Rule 1.4
  - Duty to Supervise: Model Rule 5.3

12

Legal Ethics and Cybersecurity

- Similar concepts apply in Canada:
  - Duty of Competence: Model Rule 3.1-2
  - Duty of Confidentiality: Model Rule 3.3-1
  - Duty to Inform Client: Model Rule 3.2-2
  - Duty to Supervise: Model Rule 6.1

13

Duty of Competence

Model Rule 1.1: "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 8: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology,** engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

14

Duty of Confidentiality

Model Rule 1.6:

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

* * *

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

15

ABA Formal Opinion 483 (10/17/2019)

Obligations of lawyer upon data breach affecting client data

- **Independent ethical obligation in addition to compliance with applicable laws (*e.g.*, 50 state breach notification laws, GDPR)**
- **Use reasonable efforts to monitor Internet-connected IT, external data sources, vendors with services relating to data.**
  - **Be able to determine that a breach occurred**
- **Act quickly to stop breach, mitigate damage.**
- **Inform client if substantial likelihood material client data involved (Duty to keep client informed of status of matter)**
- **Consider developing incident response plan, but not required**
  - **You need one!**
- **No duty to inform former clients except as per applicable law**
  - **Avoid retaining former client data. Have agreement on disposition**

16

1.1+1.6=Duty to Understand Confidentiality Risks of Technology

Know what you don't know and get help:

"If a lawyer is not competent to decide whether use of a particular technology (*e.g.,* cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer."

– ABA Cybersecurity Handbook

5.5 Competent Use of Information Technologies

Lawyers should have a reasonable understanding of the technologies used in their practice or should have access to someone who has such understanding.

– Law Society of Ontario's Technology Practice Management Guidelines

17

"Bank's lawyer mistakenly releases data on 50,000 accounts"

- July 2017: Wells Fargo lawyer used e-discovery software to produce documents
  - Did not realize the view she was using showed only some documents
  - Did not understand steps needed to complete redaction
  - Produced personal data, social security numbers, portfolio details on 50,000 high net worth clients to plaintiff's counsel.
  - Documents reviewed and redacted were produced unredacted

18

Unsecured Amazon Web Services S3 Buckets

- Amazon Web Services' Simple Storage Service (S3)
  - "a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web"
- Amazon makes both static and in-transit encryption available
  - But users don't always activate encryption, other security
- A new free application is available to locate unsecured S3 buckets – the bad guys will find yours!
- Essential to manage access settings, enable encryption, and make sure third parties do so too!
- You need to understand the tools you use, and understand when you don't understand!

19

Legal Technology Safeguards

- Apply duty to common legal technology:
  - Smartphones–encrypted? Password? Biometrics?
  - Laptops/tablets–encrypted? Password? Biometrics?
  - USB drives – Encrypted? Approved by IT?
  - Cloud storage/remote access tools
    - end-to-end encryption
    - Limit vendor access
  - Wireless networks
    - Public or private? Secure your home network!
- ICO Mobile Device Case

20

Cloud computing due diligence guidelines

At a minimum, consider:

- ***Confidentiality and privilege must be protected***
- **Where** is the data is stored/hosted ?
- **Who** owns the data? **Who** has access to it?
- Consequences of **seizure/destruction** of servers, or service provider going **out of business**
- **Access** to records/source code/software
- Ability to **migrate** the data
- **Laws, contracts** governing the services
- **Archive**
- **Ensuring destruction** of data when needed
- **Remedies** for non-compliance: terms/privacy policy/security promises
- Electronic **discovery**/forensic **investigation**

21

Reasonable Protection of Information

Comment 18 to Model Rule 1.6:

". . . Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to,

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

But in the end, it's up to the client!

22

Reasonable Protection of Information

- NYSBA Ethics Opinions 842 (online storage), 1019 (remote access), 1020 (cloud storage)
  - Reasonable protection of confidential information or informed client consent
  - Continued monitoring of technological advances to ensure continued adequacy of protection
  - Continued monitoring of privilege law to ensure no waiver of privilege from use

23

Implications of Comment 18: Balance

- Unencrypted email is not necessarily a violation of Model Rule 1.6. But consider:
  - Sensitivity of information
  - Likelihood of disclosure without safeguards
- MA rule: Do not send confidential communications to individual client's work email. Good idea generally!
- Need to consider content held by third-party vendors, e.g. e-discovery, accounting, data rooms
  - Security
  - Confidentiality
  - Limited access

24

NY SHIELD Act

- The Stop Hacks and Improve Electronic Data Security Act
  - Legislative staff does no have enough to do
- By March 21, 2020 any person or business with private information of NY residents must adopt a Cybersecurity Program to reduce risks of a data breach.
- Small business (<50 employees, <$3MM revenue, <$5MM assets) may adopt reasonable safeguards appropriate based on business size and complexity and sensitivity of data
- Need administrative, technical and physical safeguards
  - Vendor diligence, contract terms
  - Employee training
  - Limit information held and for how long
- Law firms will have to comply, as will their clients

25

Reasonable Protection of Information

- No specific comment on protection of information under Canadian Model Code of Professional Conduct.
- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to Canadian lawyers:

Safeguarding personal information

- PIPEDA requires personal information to be safeguarded at all times
- Security/Encryption on devices
- Care when working in public spaces or devices
- Written agreement with third party processing information (including cloud computing service providers)
- Lawyers accountable for information transferred to third party processing
- Transparency

26

Duty to Inform

Model Rule 1.4:

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

- Security measures to be taken
  - Client needs to understand risks of unencrypted email, cloud storage, vendors
- When a breach occurs
  - Client needs to be able to comply with industry regulations (e.g., health, financial services), state notification laws, etc.

27

Duty to Inform

(CAN) Model Code of Professional Conduct*:*

3.2-2 When advising a client, a lawyer must be honest and candid and must inform the client of all information known to the lawyer that may affect the interests of the client in the matter.

(QC) Code of Professional Conduct of Advocates :

37. A lawyer must be honest and candid when advising clients.

28

Data Breach Reporting and Notification

- 50 different state laws
- Usually mandatory under the GDPR
- Other global requirements
- Mandatory in Canada Pursuant to PIPEDA as of November 1, 2019
- Conceiving and testing a data breach protocol to be implemented by the organization is key
  - Very short timeline under GDPR = 72 hours
  - Under PIPEDA: Prompt notification. Late notice of breach part of claims in privacy class actions.

29

Duty to Supervise

Model Rule 5.3: "With respect to a nonlawyer employed or retained by or associated with a lawyer:

"(a) a partner, 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 the person's conduct is compatible with the professional obligations of the lawyer;"

- *Corporate Counsel, outside counsel*
- *Employees, Vendors*

30

Duty to Supervise

(CAN) Model Code of Professional Conduct*:*

6.1 SUPERVISION

Direct Supervision Required

6.1-1 A lawyer has complete professional responsibility for all business entrusted to him or her and must directly supervise staff and assistants to whom the lawyer delegates particular tasks and functions.

(QC) Code of Professional Conduct of Advocates :

5. A lawyer must take reasonable measures to ensure that every person who collaborates with him when he engages in his professional activities and, where applicable, every firm within which he engages in such activities, complies with the *Act respecting the Barreau du Québec* (chapter B-1), the *Professional Code* (chapter C-26) and the regulations adopted thereunder.

31

Employee Training is Key

- Given persistence of threats and attacks, and ethical duties, lawyers and staff all need to receive cybersecurity training. *See DLA Piper*
- Purpose is to teach all to recognize phishing, spearphishing, smishing attacks designed to gather valuable information or introduce malware. One mistake compromises the firm.
  - Ransomware – DLA Piper had no email, phones, computers for a week, weeks to recover data due to NotPetya. Somebody clicked.
  - System access
  - Objectives include extortion, insider information, IP
- Law firms and law departments are target-rich environments. Protect yourself!

32

Law Firms & Data Privacy Compliance GDPR

- The GDPR is a substantial expansion of data privacy law in the European Union (EU).
- The GDPR governs the control and processing of the personal data of individuals in the EU.
- Regulation took effect on May 25, 2018.
- **Potential fines for non-compliance are hefty: Up to €20 million or 4% of annual worldwide revenue, whichever is greater.**
- Recent fines against Google ($57M), Marriott ($124m) and British Airways ($230M).

33

Law Firms & Data Privacy Compliance GDPR

- GDPR's scope and requirements are deep and complex, so who needs to comply?
  - Organizations within the EU
  - Organizations outside the EU that offer goods and services to individuals in the EU
  - Law firms with EU clients (whether or not they have an office in the EU)
  - Law firms with EU offices or even a single lawyer representing the firm in the EU

34

Law Firms & Data Privacy Compliance
GDPR – Ask Yourself

- What is our data footprint in EU (*e.g.*, employees, clients)?
- Have we defined a GDPR compliance roadmap?
- Can we provide evidence of GDPR compliance to EU regulators, who may request it on demand?
- Do we know and control what personal data is collected, how it is used and to whom it is shared?
- Do we have compliance plan on regular assessments, documentation and escalation paths?
- Have we tested our breach-response plan to ensure it meets GDPR's 72-hour notification requirement?
- Have we identified a Data Protection Officer (DPO) if required?
- Do we need a Data Protection Representative in Europe/
- Do we have a cross-border data transfer strategy?

35

Law Firms & Data Privacy Compliance
GDPR – What can you do?

- **Strategy and governance** - Define a governance structure for your privacy program with roles and responsibilities designed to coordinate, operate and maintain the program.
- **Policy management -** Privacy policies, notices, procedures and guidelines are formally documented and consistent with applicable laws and regulations.
- **Cross-border data transfer** - Determine cross-border data transfer strategy based on current and future planned data collection, use and sharing.
- **Data lifecycle management** - Create ongoing mechanisms to identify new personal data processing and use activities, and implement appropriate checkpoints and controls.
- **Individual rights processing** - Enable the effective processing of consent and data subject requests, such as data access, deletion and portability.
- **Third parties** – Review agreements with third party service providers, affiliated firms and clients located in the EU to ensure compliance with GDPR requirements.

36

Law Firms & Data Privacy Compliance
GDPR – What can you do? Cont'd

- **Privacy by design** - Develop a strategy and playbook for "privacy by design" to incorporate privacy controls and impact assessments throughout the data lifecycle for new and changing data use initiatives.
- **Information security** -Identify existing security information protection controls and align security practices with GDPR considerations.
- **Privacy incident management** -Align incident response processes with GDPR specifications and reporting requirements. Establish a triage approach to evaluating potential privacy breaches and incidents.
- **Data processor accountability** -Establish privacy requirements for third parties to mitigate risks associated with access to the organization's information assets.
- **Training and awareness** -Define and implement a training and awareness strategy at the enterprise and individual level.

37

Asia Regional Law

- **Japan:** transfer out only to adequate jurisdiction, or with contractual obligations, or consent. No required breach notification.
- **Korea:** separate consent required to transfer out; 24-hour breach notification.
- **China:** must notify of individual and gov't when identifying a security flaw. Data localization for critical information. 4'17 draft amendment would expand.
- **Vietnam:** effective 1'19. Notice required for transfer out. Data localization for internet services, including having local representative.
- **Thailand:** effective 5'20. Consent required to transfer out. May need local rep.
- **Singapore:** cross-border transfer requires PDPC approval or contractual obligation on receiving party.
- **Philippines:** effective 3'18. Consent required for transfer out, along with contractual obligations. 72-hour breach notice required in certain situations.
- **India:** Draft law of 7'18 has data localization requirement, but proposed amendment to limit to critical data. Penalties of 4% global turnover proposed.
- **Australia:** informed consent & contractual obligations needed to move data out of country. 30 day breach notification.

38

Other Ethical Issues To Consider in Technology

- **Ability to consent to giving your personal data away –** EU seems to say no unless 'essential to the service'
- **Use of big data analytics –** Cambridge Analytica
- **Rights and Responses to a Hack –** should there be a Digital Geneva Convention?
- **Accuracy of AI Algorithms –** how to ensure automated decisions are made fairly
- **Use of technology to unfairly control populace –** Facial recognition, China
- **Cross-Border Application of Law –** Cloud Act

Jonathan Armstrong – Cordery
jonathan.armstrong@corderycompliance.com

Atsusi Okada – Mori, Hamada & Matsumoto
atshushi.okada@mhmjapan.com

Diane O'Connell – PricewaterhouseCoopers
diane.oconnell@ocolegal.com

Drew Jaglom – Tannenbaum Helpern Syracuse & Hirschtritt LLP
jaglom@thsh.com

Mary Fernandez – Headrick Rizik Alvarez & Fernandez
mfernandez@headrick.com.do

Scott Warren – Squire, Patton & Boggs
scott.warren@squirepb.com