PROGRAM MATERIALS
Program #2940
February 13, 2019

Ethics and Cybersecurity: A Lawyer's Professional Obligations Under the ABA Model Rules

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Ethics and Cybersecurity: A Lawyer's Professional Obligations Under The ABA Model Rules and ABA Formal Opinions 483, 477R, and 99-413

David Zetoony

David.Zetoony@bryancave.com

Partner, Bryan Cave LLP

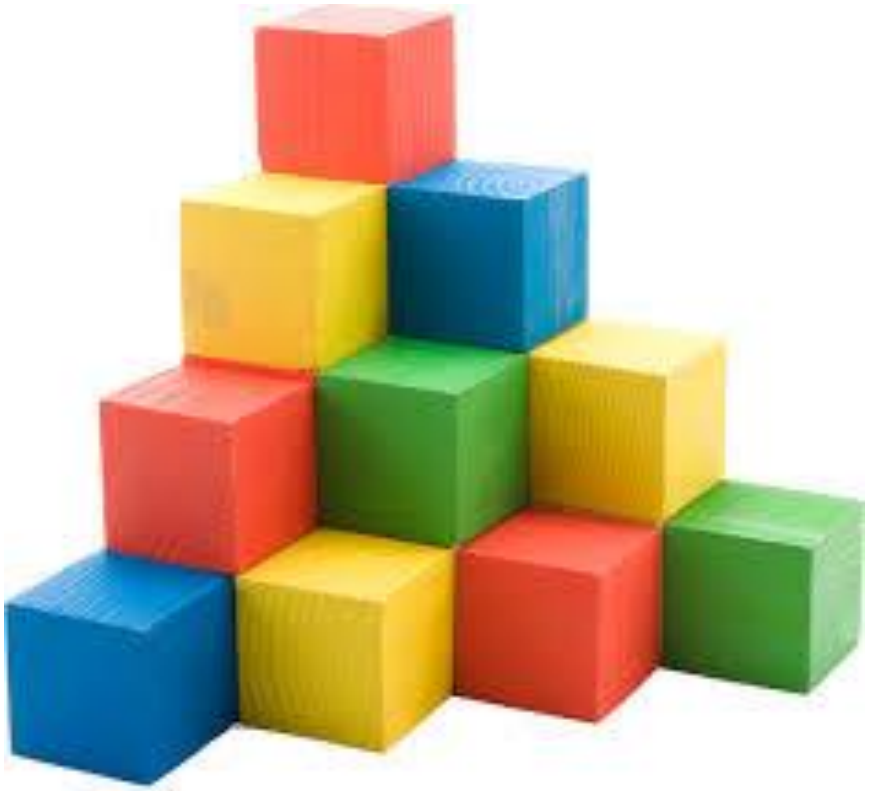
Chair Data Privacy and Security Practice

bclplaw.com

The Overarching Theme of Ethics and Cybersecurity

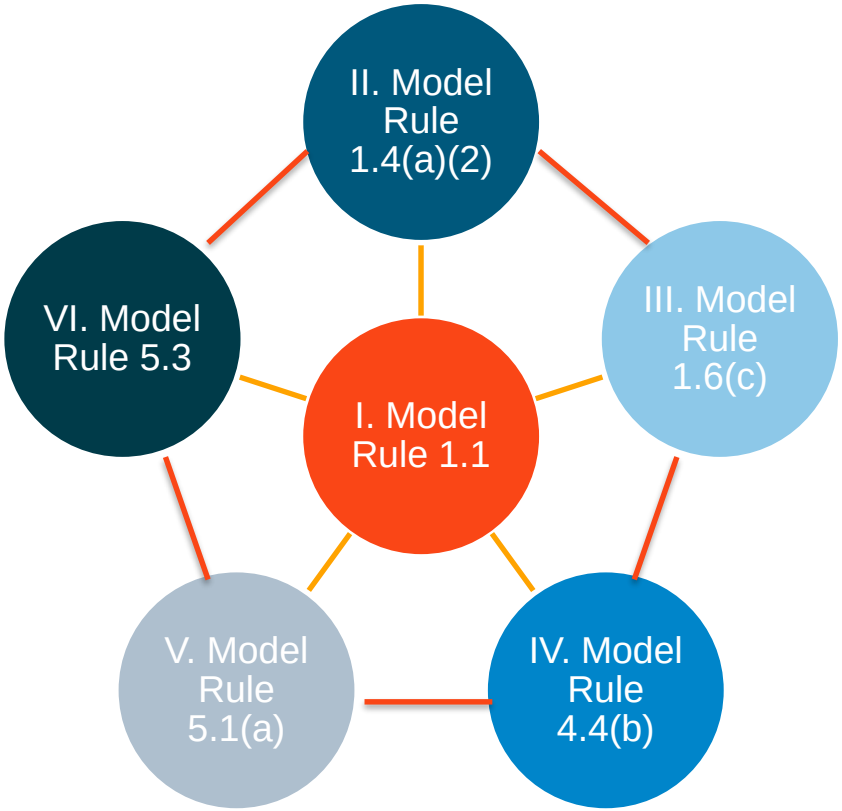
The Overarching Theme of Ethics and Cybersecurity

- There is no “cybersecurity” ethics rule.
- Instead, existing ethics rules are used as building blocks to address data security issues.



Overview of Program

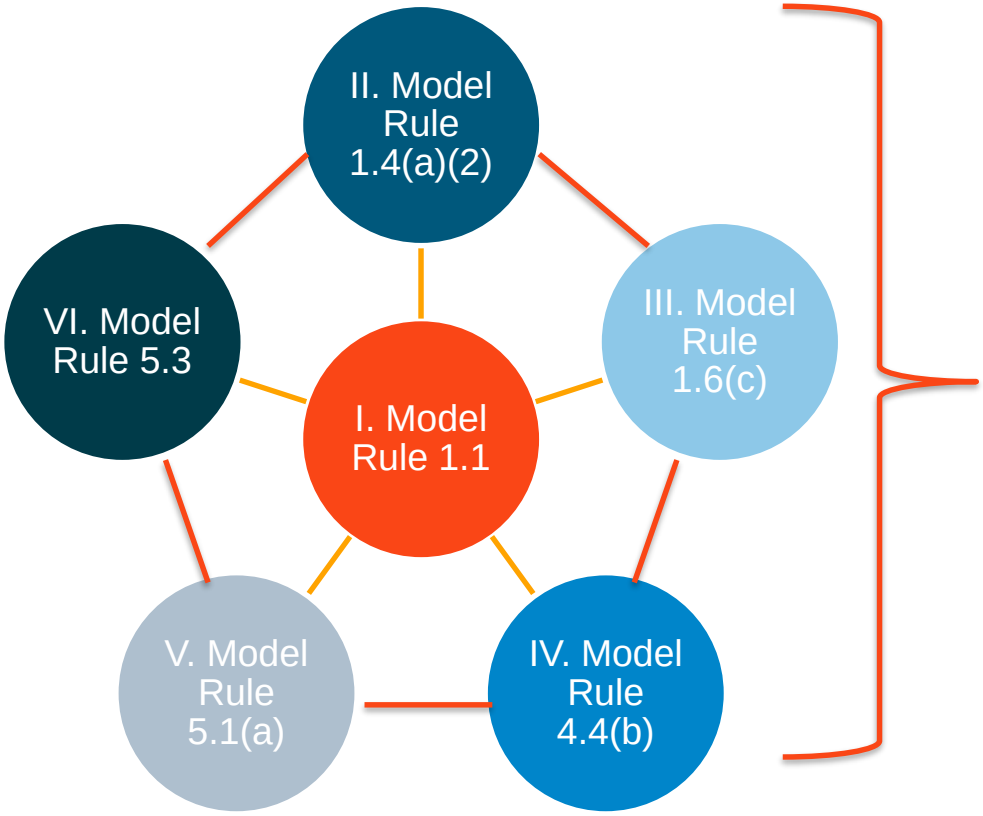
The building blocks:



BRYAN CAVE LEIGHTON PAISNER BCLP

Overview of Program

The building blocks:



Practical Impacts:

Discussion Point 1: Use of Email

Discussion Point 2: Breach Notification

BRYAN CAVE LEIGHTON PAISNER

I. Model 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." See *also* Virginia Rules of Professional Conduct 1.1.

I. Model Rule 1.1

Competence

- Comment 8 to the Rule discusses the obligation to "maintain competence" and read:

  "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

- In 2012, Comment 8 was revised to refer to technology:

  "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." Accord Virginia Rule of Professional Conduct 1.1, Comment 6.

- Note that not all states may have adopted this comment. For example, although the ABA approve the amendment in 2012 it was only recently adopted by Virginia on March 1, 2016.

I. Model Rule 1.1

Competence

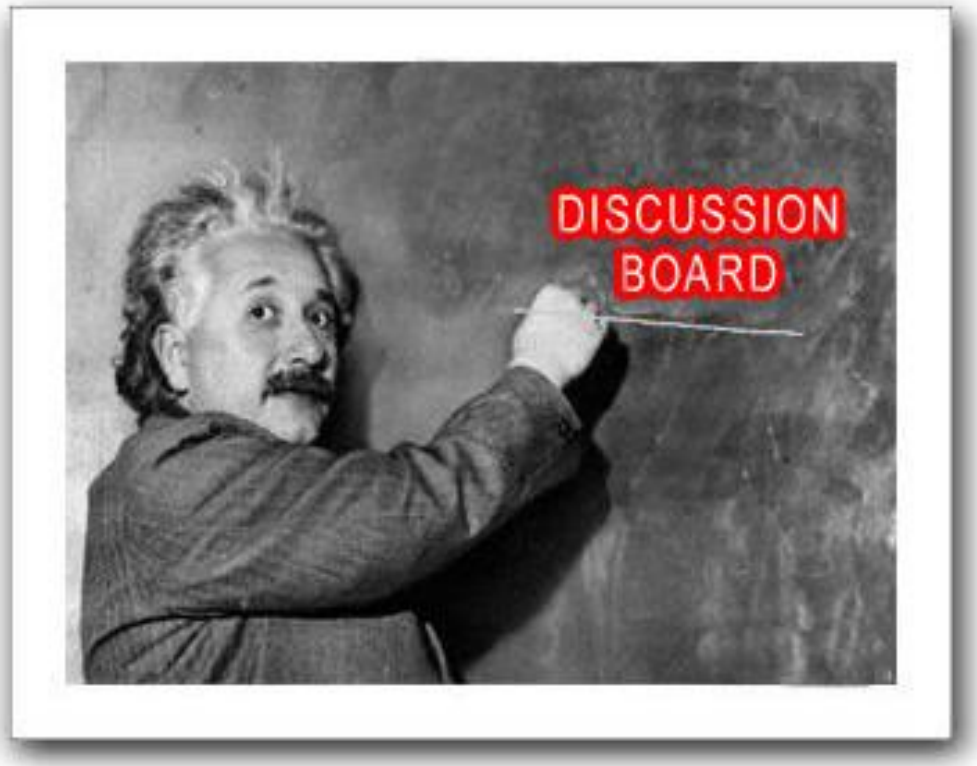
- Net result is that a lawyer must understand benefits and risks of technology

II. Model Rule 1.4(a)(2)

Communication

"A lawyer shall . . . reasonably consult with the client about the means by which the client's objectives are to be accomplished"

Model Rule 1.4(a)(2)



BRYAN CAVE LEIGHTON PAISNER BCLP

II. Model Rule 1.4(a)(2)

Communication

- Traditional notions of this rule:
  - Discuss strategy (e.g., file a motion to dismiss or not)
  - Notify client of actions taken on their behalf (e.g., communications with opposing counsel concerning settlement).
- Potential modern notions of this rule:
  - If the "means" by which the representation is going to be accomplished include technological infrastructure that may need to be conveyed.
  - For example:
    - The use of secure "document rooms" to house M&A information.
    - The use of encrypted means of communication.
    - The use of outsourced vendors to host data or host information or accomplish document reviews.
- But note, some states have not adopted Model Rule 1.4(a)(2). For example, Virginia Rules of Professional Conduct 1.4 requires that a lawyer keep a client informed of the status of a matter, comply with information requests from a client, explain a matter to a client to enable the client to make decisions, and inform client of pertinent facts and communications from opposing counsel. It does not contain a general requirement to discuss the "means" of accomplishing the representation.

II. Model Rule 1.4(a)(2)

Communication

Net Result is that Model Rule 1.4 encourages lawyers to have conversations with their clients to discuss *how* a representation will be accomplished. The "how" may include the lawyer's use of security.

III. Model Rule 1.6(c)

Confidentiality

Originally:

> "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)."

III. Model Rule 1.6(c)

Confidentiality

Added as a new subsection (c) in 2012:

> "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."
>
> See *also* Virginia Rule of Professional Conduct 1.6(d).

III. Model Rule 1.6(c)

Confidentiality

- Some states have affirmatively stated that a lawyer that takes **reasonable measures** to protect information is not subject to disciplinary action.
- For example, comment 20 to Virginia's rule states:

  "a lawyer is not subject to discipline under this Rule if the lawyer has made **reasonable efforts** to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information. Perfect online security and data protection is not attainable. Even large businesses and government organizations with sophisticated data security systems have suffered data breaches."

III. Model Rule 1.6(c)

Confidentiality

- What is Reasonable?

III. Model Rule 1.6(c)

Confidentiality

Comment 18:

"The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. **Factors to be considered** in determining the reasonableness of the lawyer's efforts include, but are not limited to,"*

1. the sensitivity of the information,
2. the likelihood of disclosure if additional safeguards are not employed,
3. the cost of employing additional safeguards,
4. the difficulty of implementing the safeguards, and
5. 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).

*Virginia also states that the "size of the firm" is one of the factors to be considered in determining what is reasonable. Virginia Rule 1.6(d), Comment 20.

III. Model Rule 1.6(c)

Confidentiality

The net result is that the type of technology that you use is a balancing test:

III. Model Rule 1.6(c)

Confidentiality

Formal Opinion 477R makes clear that the balancing test is constantly shifting:

> ". . . Lawyers must, on a case-by-case basis, **constantly analyze** how they communicate electronically about client matters, applying the Comment 18 [to Rule 1.6] factors to determine what effort is reasonable."

III. Model Rule 1.6(c)

Confidentiality

Formal Opinion 477R also recommended that lawyers consider whether to use some common forms of technology such as:

- Secure network communication (e.g., VPN)
- Passwords are (a) unique, (b) complex, and (c) rotated.
- Firewalls
- Anti-virus.
- Security patches applied.
- Remote disablement of mobile devices.
- Encryption at rest
- Multi-factor authentication.
- Data minimization

III. Model Rule 1.6(c)

Confidentiality

Other states have formalized these types of recommendations in their comments to the state rules of professional conduct:

- For example, in 2016 Comment 21 to Virginia Rules of Professional Conduct were revised to state:

  Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:

  - *(a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security; [**Training**]*
  - *(b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data; [**De-provisioning**]*
  - *(c) Procedures addressing security measures for access of third parties to stored information; [**Encryption; Access controls**]*
  - *(d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused; [**Disposal**]*
  - *(e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and [**Passwords**]*
  - *(f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity. [**IPS / IDS / Antivirus**]*

III. Model Rule 1.6(c)

Confidentiality

You do not have to conduct the "reasonableness" balancing test alone. Some states have also specifically stated that lawyers are not expected to become technology experts and may (or should) turn to consultants:

> *"To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer* ***can and more likely must turn to the expertise of staff or an outside technology professional****. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well*."
>
> Comment 20 to Virginia Rule of Conduct 1.6(d).

III. Model Rule 1.6(c)

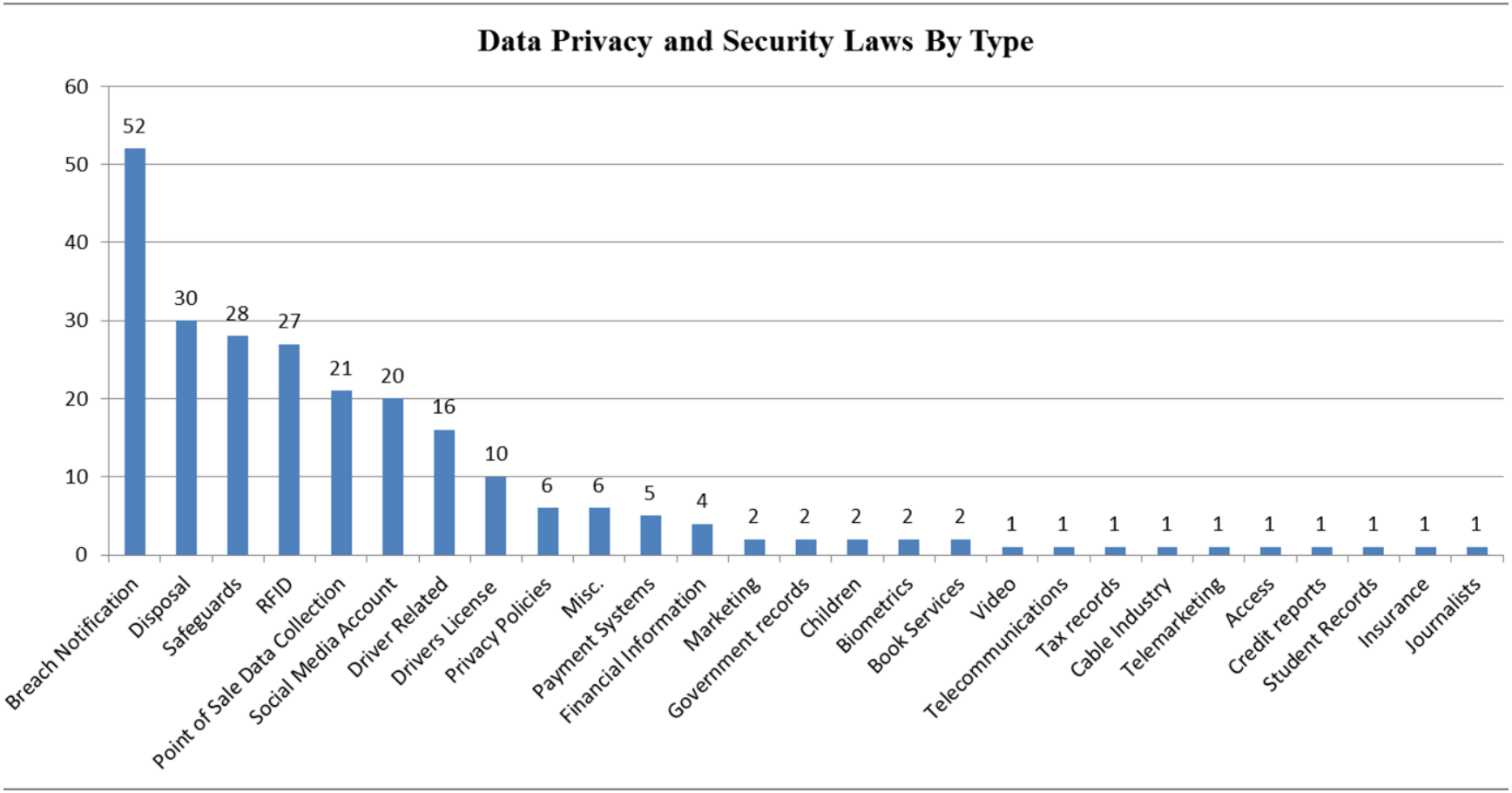
Confidentiality

It is important to note that the standards set forth in Rule 1.6(c), ABA Comment 18, and state equivalents are just the floor. As Comment 18 notes:

> "Whether **a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy** or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, **is beyond the scope of these Rules**. "

III. Model Rule 1.6(c)

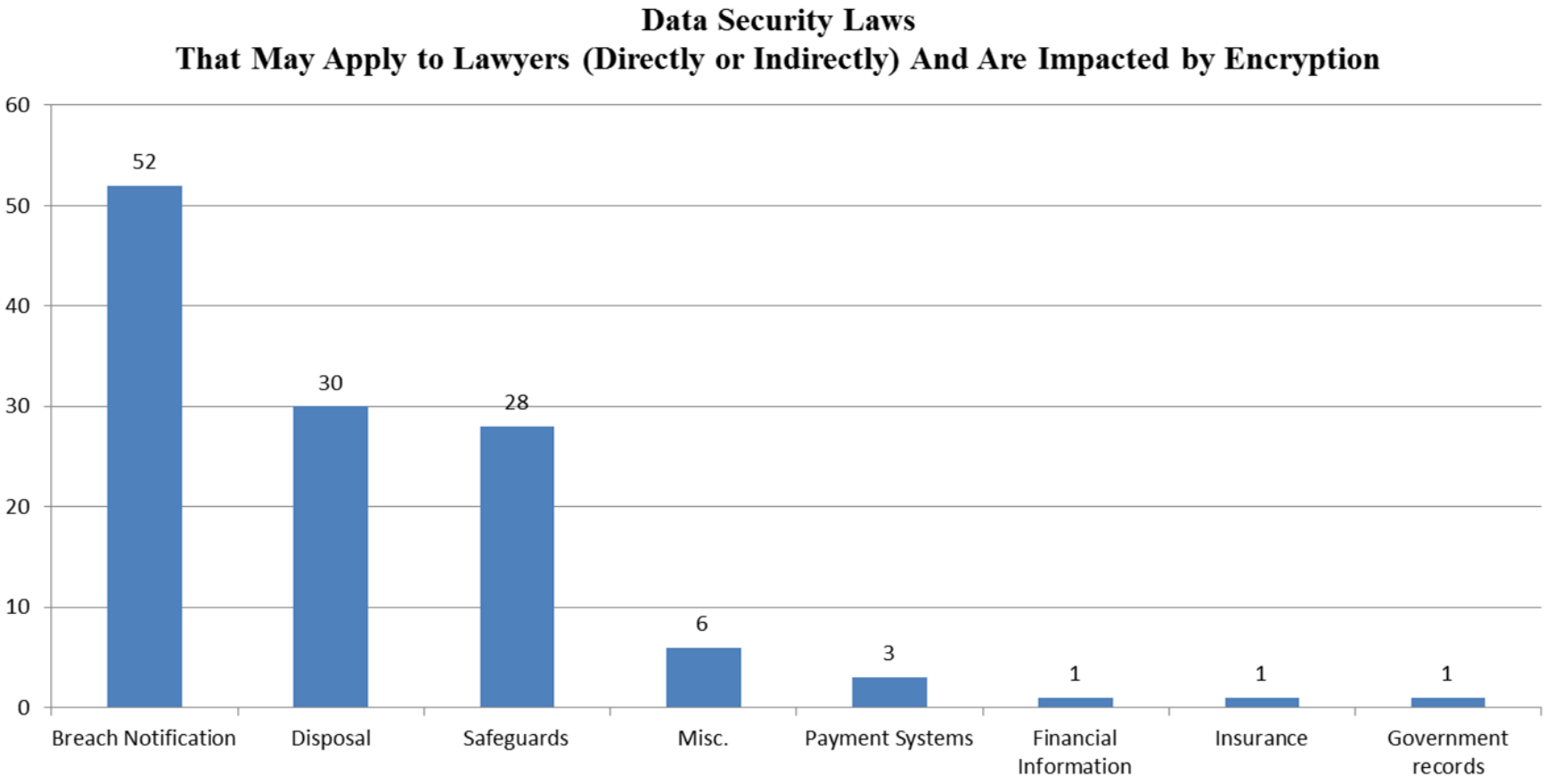
Confidentiality



BRYAN CAVE LEIGHTON PAISNER BCLP

III. Model Rule 1.6(c)

Confidentiality



BRYAN CAVE LEIGHTON PAISNER BCLP

III. Model Rule 1.6(c)

Confidentiality

- There is no one data security or data privacy law.
- There are ~300 data privacy and security laws (federal and state) in the US.
- Passed at different times, different jurisdictions, different legislatures, different priorities, different political environments.
  - Lack cohesiveness in terms of:
  - Requirements
  - Scope
  - Penalties

III. Model Rule 1.6(c)

Confidentiality

Primary Federal Laws

1. The Federal Trade Commission Act. 15 B.SC.. 41, et seq. The FTC has attempted to fill a perceived void in federal omnibus legislation by using the Federal Trade Commission Act's ("FTCA") prohibition on "unfair or deceptive practices."
   - "Deception" actions focus on statements that a company has made about its security.
   - "Unfairness" actions take the position that it is inherently unfair to take consumer information if appropriate security is not applied.
   - The FTC has primarily used its data security authority in the context of negotiated consent orders. Some commentators have argued that the agreements that have arisen from those orders have formed a type of jurisprudence by acclamation or a road-map of required security practices.
   - FTC consent orders suggest that the following practices are part of a "reasonable" program:
     1. Password Protection
     2. Encryption
     3. Limited Access
     4. Limited Data Retention
     5. Data Disposal

III. Model Rule 1.6(c)

Confidentiality

Other Primary Federal Laws (Cont.)

2. Health Insurance Portability and Accountability Act ("HIPAA"). 45 COFFER. 164, et seq.
3. Gramm-Leach-Bliley Act ("GALBA"). 15 B.SC.. 6801, et seq.; 16 CFR 313.1, 314.1.

Primary Federal Laws (Cont.)

1. State Consumer Protection Acts. State general consumer protection statutes mimic the data security jurisprudence of the FTC. As a result, as the FTC establishes precedent under "deception" and "unfairness" theories similar cases can be brought under many state statutes.

2. Data Breach Notification Statutes. 47 states, the District of Columbia, and various US territories have enacted data breach notification statutes. Although the statutes differ in substance, they generally require that a company notify affected state residents (and in some instances state regulators) if the company becomes aware that sensitive personal information about a state becomes acquired and/or is accessed by an unauthorized third party.

III. Model Rule 1.6(c)

Confidentiality

Other Primary State Laws (Cont.)

3. State Data Safeguards Statutes. Some states, most notably Massachusetts have statutes that require that companies take steps to protect sensitive personal information.

4. Data Disposal Statutes. A number of states have enacted statutes requiring companies that collect certain types of information (e.g., social security numbers) to properly dispose / delete that information when the information is no longer necessary.

IV. Model Rule 4.4(b)

Respect for Third Person Rights

"A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."

IV. Model Rule 4.4(b)

Respect for Third Person Rights

What is the implication of this rule to cybersecurity? Make sure that you mark all documents that are sent externally with appropriate legends so that the receiving party "knows or reasonably should know" that the documents are confidential and/or privileged.

- Note that this Rule does not require that the receiving party return the documents to you. See Comment 2 of Rule 4.4(b).
- Note that this Rule also does not guarantee that privilege is protected as a result of the inadvertent disclosure. *Id*.
- It does ensure that if your documents are appropriately marked that you will be told of the disclosure if the recipient is a fellow attorney.

V. Model Rule 5.1(a)

Responsibilities of a Supervising Attorney

"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."

V. Model Rule 5.1(a)

Responsibilities of a Supervising Attorney

What is the implication of this rule to lawyers?

- Obligation of partners / managers of a firm to bring the firm into compliance with cybersecurity obligations.
- Obligation of partners / managers of a firm to train those attorneys who they supervise with regard to the proper handling of information.

VI. Model Rule 5.3

Responsibilities Regarding Non-Lawyer Assistance

“ With respect to a nonlawyer employed or retained by or associated with a lawyer . . . 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”

VI. Model Rule 5.3

Responsibilities Regarding Non-Lawyer Assistance

ABA Formal Opinion 08-451 identified several issues that a lawyer should consider when selecting a service provider / outsource vendor including, among other things:

1. Reference checks and vendor credentials
2. Vendor's security policies and protocols
3. Vendor's hiring practices
4. Use of confidentiality agreements

Practical Impact Discussion Point #1: Email Communication

Remember 1999?

Euro was first introduced as a currency

Bill Clinton was acquitted

Google was a few months old

Email was just starting to take over as a mainstream form of business communication

Practical Impact Discussion Point #1: Email Communication

ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 99-413 (Mar. 10, 1999) to address whether lawyers should use email in their practices:

- Focused almost exclusively on Rule 1.6(a)'s requirement that lawyers take "reasonable steps" to prevent unauthorized disclosure.
- In analyzing whether the use of email was a reasonable step it compared the risks incumbent with email to those of traditional forms of communication (E.g., US mail, landline telephones, cell phones, and faxes). It found that all raised similar possibilities that information may be lost.

Practical Impact Discussion Point #1: Email Communication

Formal Opinion No. 99-413 (Mar. 10, 1999) Cont.:

	US Mail	Landline	Cell	Fax	Email
Is access by the carrier possible?	Yes.	Yes.	Yes.	Yes.	Yes.
Are there laws that prohibit third party interception?	Yes.	Yes.	Yes.	Yes.	Yes.
Can it be easily tapped with little sophistication?	No (because letters are sealed).	Yes.	Yes (analog technology)	Yes	No (Because of transmission in packets).
Are multiple people involved in transmission?	Yes (implicit in the opinion)	No	No	Yes.	No.

Practical Impact Discussion Point #1: Email Communication

Fast forward to 2017 and the ABA Standing Committee on Ethics and Professional Responsibility re-evaluated the permissibility of using email in Formal Opinion 477R. The Committee evaluated the six rules discussed above.

Practical Impact Discussion Point #1: Email Communication

Formal Opinion 477R:

- Rule 1.1 (requirement to evaluate benefits and risks of technology)
  - The Rule requires that lawyers must keep abreast of the relevant risks involved with email.
- Rule 1.4 (requirement to discuss security with clients)
  - The Rule requires that lawyers discuss security with clients, including, for example, when encrypted communications should be used instead of clear-text email.
  - If a lawyer believes that highly sensitive information is being transmitted, the lawyer should inform the client about the risks of clear text transmission, and the lawyer and client "should decide whether another mode of transmission . . . is warranted."

Practical Impact Discussion Point #1: Email Communication

Formal Opinion 477R:

- Rule 1.6(C) (requirement to make reasonable efforts to prevent disclosure). Suggests that the following might be a baseline of reasonable:
  - Secure network communication (e.g., VPN)
  - Passwords are (a) unique, (b) complex, and (c) rotated.
  - Firewalls
  - Anti-virus.
  - Security patches applied.
  - Remote disablement of mobile devices.
  - Encryption at rest
  - Multi-factor authentication.
  - Data minimization

Practical Impact Discussion Point #1: Email Communication

Formal Opinion 477R:

- Rule 4.4(b) (requirement to notify opposing counsel if he receives a document that he knows he should not)
  - "Lawyers should follow the better practice of marking privileged and confidential client communications as "privileged and confidential""
  - "This can also consist of something as simple as appending a message or "disclaimer" to client emails, where such a disclaimer is accurate and appropriate for the communication."

Practical Impact Discussion Point #1: Email Communication

Formal Opinion 477R:

- Rule 5.1 (requirement that partners and supervisors make reasonable efforts to ensure firm compliance with rules)
  - "lawyers must establish policies and procedures,"
  - "lawyers must . . . periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients."
  - "Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. "
  - "Supervising lawyers must follow up to ensure these policies are being implemented "
  - "partners and lawyers with comparable managerial authority must periodically reassess and update these policies."

Practical Impact Discussion Point #1: Email Communication

Formal Opinion 477R:

- Rule 5.3 (requirement that lawyers make a reasonable effort to make sure that non-lawyer (e.g., secretaries, service providers) conduct is compatible with rules).
  - Rule 5.1 supervision requirements are extended to non-lawyers.

Practical Impact Discussion Point #2: Data Breach

- Formal Opinion 483 (Oct. 17, 2018) “Lawyer’s Obligations After an Electronic Data Breach or Cyberattack.”
  - Ethical obligations are independent of legal obligations. As a result “lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.”
  - In relation to Ethics…

Practical Impact Discussion Point #2: Data Breach

- **Obligation to monitor systems for breaches**
  - Committee read an obligation for lawyers and law firms "to monitor the technology and office resource connected to the internet, external data sources, and external vendors" for a data breach.
  - The origins of this obligation are not entirely logical, but the Committee asserts the obligation flows from Model Rule 5.1(a) and 5.3:

V. Model 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."

VI. Model Rule 5.3

" With respect to a nonlawyer employed or retained by or associated with a lawyer . . . 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"

Practical Impact Discussion Point #2: Data Breach

- **Obligation to Stop the Bleeding.**
  - Committee read an obligation for lawyers and law firms to "stop the breach and mitigate damage resulting from the breach" as flowing from 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."

- Presumably the Committee's thinking is based on the premise that you can't represent a client effectively if you are actively losing data or your systems are compromised.
- Committee recommended "proactively developing an incident response plan with specific plans and procedures for responding to a breach."

Practical Impact Discussion Point #2: Data Breach

- **Obligation to Restore Systems**.
  - Committee interprets Rule 1.6(c) as requiring a lawyer to restore their systems quickly "to be able again to service the needs of the lawyer's clients."

III. Model Rule 1.6(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."

Practical Impact Discussion Point #2: Data Breach

- **Obligation to Notify Clients**. Committee interprets Rule 1.4 as requiring a lawyer to "communicate with current clients about a data breach."

II. Model Rule 1.4(a)(2)

"A lawyer shall . . . reasonably consult with the client about the <u>means by which the client's objectives are to be accomplished</u>" Model Rule 1.4(a)(2)

Practical Impact Discussion Point #2: Data Breach

- Surprisingly….
  - Committee did not find there to be an ethical obligation to notify former clients that were impacted by the breach: “The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.”
  - Committee did not address the dilemma that many lawyers may face after a breach where they may be legally obligated to notify data subjects *but* ethically obligate to keep their clients’ confidence

Practical Impact Discussion Point #2: Data Breach

- Surprisingly….
  - For example, under the European General Data Protection Regulation (“GDPR”) if a controller (and most lawyers are considered controllers) suffers a data breach they are required to notify data subjects (i.e., those whose information was breached) if the breach “is likely to result in a high risk to the rights and freedoms of natural persons.” The obligation to notify an impacted individual could easily conflict with the ethical obligation of confidentiality imposed by Model Rule 1.6

David A. Zetoony
Bryan Cave LLP
Boulder CO / Washington DC

Phone: 202 508 6030
Fax: 202 220 7330
Email: david.zetoony@bryancave.com

David Zetoony is the leader of the firm's global data privacy and security practice. He has extensive experience advising clients on how to comply with state and federal privacy, security, and advertising laws, representing clients before the Federal Trade Commission, and defending national class actions. He has assisted hundreds of companies in responding to data security incidents and breaches, and has represented human resource management companies, financial institutions, facial recognition companies, and consumer tracking companies before the Federal Trade Commission on issues involving data security and data privacy.

BRYAN CAVE LEIGHTON PAISNER BCLP

bclplaw.com