ANCIENT FOUNDATIONS AND MODERN EQUIVALENTS VI
ETHICS AND PROFESSIONALISM IN GEORGIA

FEBRUARY 13, 2020

Co-Sponsors Georgia State Bar Business Law Section and
The Michael C. Carlos Museum, Emory University

Data Privacy, Cybersecurity and the Rules of Professional Conduct: Digital Ethics for Modern Lawyer

Privacy Updates:

A. California Consumer Privacy Act (CCPA).

The California Consumer Privacy Act ("CCPA") went into effect on January 1, 2020, Cal. Civ. Code §§ 1798.100 to 1798.199. However, the California Attorney General stated that he does not intend to bring enforcement actions for violations until July 1, 2020, except for egregious of violations.

The CCPA protects California residents. When the law was first enacted, it was unclear whether it applied to employees. There were debates on its applicability to employees and requests for clarification. On October 11, 2019, California's Governor Gavin Newsom announced that he signed five (5) amendments to the CCPA, including a provision that CCPA did apply to employees. However, there is a one (1) year exception that limited California employees' rights for that first year. During that limited time, they have the right to know what personal information their employers have about them and what they do with it.

The CCPA applies to a business if:

(1) it is a for-profit legal entity;

(2) that collects consumers' personal information on its own or by others on its behalf;

(3) that alone or jointly with others determines the purposes and means of processing;

(4) that "does business" in California; AND

(5) satisfies at least ONE of the following:

(a) has annual gross revenues in excess of $25 M;

(b) annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices; OR

(c) derives 50% or more of its annual revenues from selling consumers' personal information.[1]

A California "consumer" is defined as a natural persons who is a California resident, which means:

(a) In California for other than a temporary or transitory purpose, OR

(b) Domiciled in California, but currently outside the state for a temporary or transitory purpose.[2]

The CCPA's protections also apply regardless of how the business identifies an individual consumer, including by any unique identifier, household, or device.

The definition of personal information is broad under CCPA. It includes any information that directly or indirectly identifies, describes, or can reasonably link to a particular consumer or household.[3] CCPA protects data even if it does not relate to a single individual, as it covers households and data, even if the data does not contain a name. Some examples of personal information include:

---

[1] Cal. Civ. Code § 1798.140(c)(1). Additionally, a "business" includes any entity that controls or is controlled by a covered business, which means: (a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business; (b) control in any manner over the election of most of the directors or of individuals exercising similar functions; (c) the power to exercise a controlling influence over the management of a company; (d) shares common branding with a covered business (e.g., shared trademark or service mark). Cal. Civ. Code § 1798.140(c)(2).

[2] Cal. Code Regs. tit. 18 § 17014.

[3] Cal. Civ. Code § 1798.140(o).

- real name;
- alias;
- postal address;
- email address;
- unique personal or online identifier;
- internet protocol (IP) address;
- account name;
- Social Security number (SSN);
- driver's license or passport number;
- Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, or other similar information;
- Professional or employment-related information;
- Educational information;
- Inferences drawn from any of the above to create a profile about a consumer.[4]

Personal information excludes:

- "Publicly available information" – information that is lawfully made available from federal, state, or local government records;

[4] Cal. Civ. Code § 1798.140(o)(1).

- "De-identified" or "aggregate" consumer information;[5]
- Information collected, used, sold, or disclosed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach Bliley, or the Driver's Privacy Protection Act of 1995, but only if CCPA is in conflict with those laws; [6]
- Information sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act), when the personal information is "reported in, or used to generate" a consumer credit report.[7]

CCPA is primarily a disclosure and transparency statute. Businesses subject to it are required to provide notice about their practices regarding the collection of personally identifiable information (or "PII"). They have a duty to disclose and keep up-to-date, at least once every 12 months, a description of consumers' rights. Businesses subject to CCPA must list separately the categories of PII collected, sold, and disclosed for a business purpose in the preceding 12 months. They must provide notice about onward transfers of PII. Further, they must make available two (2) or more designated methods for requesting PII held by the business.

The main requirements of the CCPA also include implementing and maintaining reasonable security measures and practices. This is also the area where a consumer may bring a private right of action for violations. If businesses are selling PII, they must:

- Provide right to opt-out via a clear and conspicuous link entitled: "Do Not Sell My Personal Information;"

---

[5] Cal. Civ. Code § 1798.140(a), (h).

[6] Cal. Civ. Code § 1798.145.

[7] *Id.*

- Seek opt-in consent from consumers between the ages of 13-16;
- Seek opt-in consent from parents if a consumer is under 13 years of age.

They must also establish procedures for receiving and processing verifiable consumer requests.

Pursuant to CCPA, consumers have various rights to control their personal information. They have the right to:

- Request disclosure of categories of PII and specific pieces of PII that the business collected on them in last 12 months;[8]
- Right of access to purposes for which PII is used and with whom it is shared;[9]
- Right of deletion;[10]
- Right to opt-out of the sale of PII;[11]
- Right to data portability;[12]
- Right to sue for data security breaches;
- Anti-discrimination for exercising rights provided by CCPA.[13]

"Sale" of PII is defined broadly. It includes any communication or transfer of PII to another business or third party for monetary or other valuable consideration. A sale could include non-cash benefits, such as the ability to target advertising to specific consumers and access to marketing list. Moreover, "sale" broadly reaches any transaction for monetary value, such as transferring, making available, disclosing, releasing, renting, etc. Cal. Civ. Code §

[8] Cal. Civ. Code §§ 1798.110(c)(1), 1798.130(a)(5).

[9] Cal. Civ. Code § 1798.110(c)(2).

[10] Cal. Civ. Code § 1798.105(b).

[11] Cal. Civ. Code §§ 1798.120(b), 1798.135.

[12] Cal. Civ. Code §§ 1798.100(a), 1798.110(a), (c), 1798.130(a)(2).

[13] Cal. Civ. Code § 1798.125(a)(1); s*ee also* Cal. Civ. Code §§ 1798.125(b) and 1798.135.

1798.140(t)(1).

There are certain exceptions to the definition of "sale." For example, there is a "service provider" exception, which provides that a business does not "sell" information if it is provided to a service provider under specific circumstances. These circumstances are that the business must: (a) share or use PII with the service provider for a business purpose; (b) have previously provided a "Do Not Sell My Personal Information" notice; and (c) the service provider does not further collect, sell, or use the consumers' personal information, except as necessary to perform the business purpose. Cal. Civ. Code § 1798.140(t)(2)(C). Additionally, there is an exception if the consumer requests that the PII be disclosed. There is an exception for mergers and acquisitions.[14]

The California Attorney General has the right of enforcement of the CCPA. In actions by the Attorney General, penalties may be imposed of up to $7,500 per intentional violation. Penalties may be imposed of up to $2,500 for unintentional violations, and there is a 30 day opportunity to cure after notice of the alleged violation. The California Attorney General also may seek an injunction.[15]

Consumers have a private right of action for security breach violations. Statutory damages range between $100-$750 per consumer, per incident, or actual damages, whichever is greater. Consumers also may seek injunctive or declaratory relief.

A number of states in the U.S. are considering and in the process of drafting and negotiating laws that are similar to CCPA. There are various versions of proposed legislation at the federal level, as well, which include various aspects and similarities to CCPA. States are not

[14] Cal. Civ. Code § 1798.140(t)(2).

[15] Cal. Civ. Code § 1798.155(b).

only influenced by CCPA, but also by the General Data Protection Regulation ("GDPR"), which is applicable with regard to the European Union and its residents.

B. General Data Protection Regulation (GDPR).

The General Data Protection Regulation went into effect on May 25, 2018. It applies to residents of the EU and the European Economic Area ("EEA"). It replaced the former Data Protection Directive (Directive 95/46/EC). Member states have a limited right to introduce more specific provisions, with Germany as an example.

A business must comply with GDPR if it is a:

(1) Controller or processor of personal information located in the EU, regardless of whether the processing takes place in EU, (GDPR, Article 3(1)); or

(2) Processor of personal information of data subjects in the EU, where the processing relates to:

(a) Offering of goods or services to data subjects in EU, regardless of whether a payment is required from data subject, (Article 3(2)(a)); or

(b) Monitoring the behavior of data subjects, as their behavior takes place in EU, (Article 3(2)(b)).

As with CCPA, GDPR defines personal data broadly. Personal information is information that can be used to identify, directly or indirectly, an individual.

For example:

- Personal details;
- Family and lifestyle details;
- Education and training;
- Medical details;

- Employment details;
- Financial details;
- Contractual details (e.g., goods and services provided to data subject);
- On-line identifiers.

Pseudonymization is processing of personal data so that it can no longer be attributed to a specific data subject. Personal data includes information that has been pseudonymized, unless it is in a form that can no longer be attributed to an individual. Any additional information that identifies the individual must be kept separate from the pseudonymized data. Pseudonymized personal data that cannot be attributed to an individual is not personal data.[16]

There are also special categories of personal data that receive additional protections under GDPR. GDPR prohibits the processing of personal data that reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for purposes of identifying individuals;
- Data concerning health; and
- Sex life and sexual orientation.

(GDPR, Article 9(1).) Processing of special categories of personal data only will be allowed where (1) the data subject has given explicit consent to processing for one or more specific purposes; (2) it is necessary for purposes of carrying out the obligations of the controller or of

[16] ***See*** Downing, Robbie, *Overview of EU General Data Protection Regulation*, PRACTICAL LAW UK PRACTICE NOTE.

the data subject in employment, social security, and social protection law; (3) it is necessary to protect the vital interests of the data subject or another individual, where the data subject is incapable of giving consent (e.g. incompetence or inability of data subject); (4) the processing is carried out: (i) by a not-for-profit entity with political, philosophical, religious, or trade union aims; (ii) with appropriate safeguards; and (iii) solely with regard to members or former members of that entity to persons who have regular contact with it; (5) relates to personal data that is manifestly made public by the data subject; (6) is necessary for establishment, exercise, or defense of legal claims, or by courts in their judicial capacity; (7) substantially in the public interest; (8) for preventative or occupational medicine; (9) interest of the public health or (10) for archiving purposes in the public interest, scientific, historical research, or statistical purposes, (GDPR, Article 9(2)).

1. Controlling Principles.

a. Lawfulness, Fairness, and Transparency.

GDPR is based on a fundamental human right to privacy. Some of the primary controlling principles of GDPR are lawfulness, fairness, and transparency. This means that personal data must be processed lawfully, fairly and in a transparent manner concerning the data subject (GDPR, Article 5(1)(a)).

Specific transparency requirements include the data subject's right to receive information:

- On the identity of the controller and the nature of the processing, (GDPR, Articles 13 and 14).
- Whether personal data is being processed, and if so, the nature and purposes of that processing, (Article 15).

- Any personal data breach when that breach is likely to result in a high risk to the data subject's rights and freedoms, (Article 34(1)).

Certain types of information are required to be provided pursuant to the transparency requirement. The information that must be supplied depends on whether the controller collects the data directly from the data subject or obtains the data from a third party. At the time personal information is collected from the data subject, the controller must provide the data subject with the following information:

- Identity and contact details of the controller;
- Contact details of the data protection officer, if applicable;
- Intended purposes of, and the legal basis for, the processing;
- Where the processing is on a legitimate interest, specify the legitimate interest pursued by the controller;
- Recipients or categories of recipients of personal data;
- Whether the controller intends to transfer the personal data to a country outside the EU, and if so, if there is an adequacy decision or information about the appropriate or suitable safeguards to secure the data, the right to receive a copy of them, and where they may be found;

Additionally, the controller must notify the data subject of:

- The period for which the data is stored, or the criteria used to determine that period;
- The data subject's right to:
    - Access personal data held (Article 15);
    - Rectification (Article 16);

- Erasure (Article 17);
- Restriction of processing (Article 18);
- Right to object to processing (Article 21); and
- Right to data portability (Article 20).

Further, where data processing is based on the data subject's consent, the controller must disclose the right to withdraw that consent at any time. It must disclose the right to lodge a complaint with the supervisory authority (SA). Data subjects also are entitled to know the existence of automated decision-making or profiling, the logic involved in this activity, and the consequences of such processing for the data subject.

With regard to data obtained from third parties, the controller must provide data subjects with the same information within a reasonable period after obtaining the personal data, up to a maximum of one (1) month. There is an exception if providing this information would involve disproportionate effort. (Article 14(3) and (5)(b)). If the personal data is used to communicate with the data subject, then the information must be provided at the time when the first communication is sent. If the controller intends to disclose the data to a third party, then the information must be provided, at the latest, when the data is first disclosed.

Lawfulness of processing involves requiring a controller to justify the processing of personal data before it will be considered lawful. A controller may only process personal data on the basis of one or more of the following legal grounds:

- The data subject has given consent to processing personal data for one or more specific purposes;
- Necessary for entering or performing a contract with the data subject;

- Necessary for compliance with a legal obligation by the controller;
- Necessary to protect the vital interests of the data subject;
- Necessary for a task carried out in the public interest or based on the exercise of official authority vested in the controller;
- Necessary based on the legitimate interests of the controller or a third party, except where these interests are overridden by the interests or the fundamental rights and freedoms of the data subject (e.g., where data subject is a child).

Unlike CCPA, which is an opt-out statute, GDPR requires that the data subject give affirmative consent to the use of personal information. Silence, pre-ticked boxes, or inactivity are not considered to be adequate consent. Examples of effective consent include: (i) clicking a box when visiting a website, and (ii) choosing a technical setting for an on-line service. Affirmative consent includes any other conduct that clearly indicates the data subject's consent for the proposed processing of his/her personal data. Data subjects have the right to withdraw consent at any time, and it must be as easy to withdraw consent as it was to give it.

With regard to children, personal data of persons below the age of 16 can only be processed based on consent if consent is given by the holder of parental responsibility over the child. Member states have the right to lower the age to 13. The controller must make reasonable efforts to verify parental consent.

b. Purpose Limitation.

Another controlling principle of GDPR is purpose limitation. Purpose limitation binds the controller to the specified, explicit, and legitimate purposes of which the data subject was notified when providing consent. (Article 5(1)(b).) It cannot be further processed in a manner incompatible with those purposes. Exceptions to this requirement are that further processing is

allowed with the data subject's consent, allowed based on the EU or member state's law, or allowed in the public interest. The public interest exception involves scientific or historical research purposes, or statistical purposes.

c. Data minimization.

A third controlling principle of GDPR is data minimization. Data minimization ensures that the personal data maintained is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed, (GDPR, Article 5(1)(c)).

d. Accuracy.

Yet another controlling principle is accuracy. Personal data must be accurate and, where possible, kept up to date, (GDPR, Article 5(1)(d)).

e. Storage limitation.

A fifth controlling principle is storage limitation. Personal data must not be kept in a form that allows identification of data subjects for longer than is necessary to achieve the purposes for which the data was processed, (GDPR, Article 5(1)(e)).

f. Integrity and confidentiality.

The sixth controlling principle of GDPR is integrity and confidentiality. Personal data must be processed pursuant to appropriate security measures (GDPR, Article 5(1)(f)). This includes protection against accidental loss, destruction or damage.

g. Accountability.

A final primary controlling principle of GDPR is accountability. This means that the controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles, (GDPR, Article 5(2)).

2. <u>Data Protection by Design and Default.</u>

GDPR encompasses the notion of data protection by design and default. This means that the controller must implement appropriate technical and organizational measures to ensure protection of personal data. By default, only personal data that is necessary for a specific purpose is allowed to be collected, stored, used, and shared.

With regard to implementing adequate security measures, the following may be considered:

- Pseudonymization and encryption of personal data.
- Confidentiality of personal data.
- Integrity, availability, and resilience.
- Restore availability and access to personal data in timely manner.
- Testing, assessing, and evaluating effectiveness of technical and organizational measures.[17]

3. <u>Data Security Breach.</u>

After the improper access to personal data in the form of a data breach, a controller is required to notify the national supervisory authority without "undue delay" and in any event within 72 hours of becoming aware of the breach, (GDPR, Article 33(1).) Additionally, processors must inform their controllers "without undue delay after becoming aware" of a breach. No notification requirement exists with regard to breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons." The notice required to a SA includes:

- The nature of the breach, including the categories and number of data subjects affected;
- Categories and approximate number of data records concerned;

[17] *See* footnote 16, *supra.*

- Identity and contact details of the DPO or other contact point where more information can be obtained;
- Consequences of the personal data breach; and
- Measures proposed or taken by the controller to address the personal data breach.

(GDPR, Article 33(3).)

Notice also must be provided to data subjects without "undue delay" if the data breach is likely to result in a high risk to the rights and freedoms of the data subjects (GDPR, Article 34(1).) The notice must clearly describe the nature of the personal data breach and contain information about:

- The identity and contact details of the DPO or other contact point where more information can be obtained;
- The consequences of the personal data breach; and
- The measures proposed or taken by the controller to address the personal data breach.

(GDPR, Article 34(2).) There is no need to inform data subjects of the breach if the controller has appropriate technical and organizational protection measures in place, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption. Moreover, the controller must have taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is not likely to materialize.

C. Rules of Professional Responsibility.

Changes in technology, in the amount and types of personal information that businesses collect, use, and sell, and the laws that have been enacted nationally and internationally to protect

such data have changed the nature of how attorneys advise their clients. These developments also have changed the way law firms conduct business themselves. The changes have impacted the Rules of Professional Conduct and how they are applied.

1. Georgia Rule 1.1, Competence.

Georgia Rule 1.1 provides:

> A lawyer shall provide competent representation to a client. Competent representation as used in this rule means that a lawyer shall not handle a matter which the lawyer knows or should know to be beyond the lawyer's level of competence without associating another lawyer who the original lawyer reasonably believes to be competent to handle the matter in question. Competence requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 6 explains that "lawyers should keep up with changes in the law and its practice, including the benefits and risks associated with relevant technology."

Lawyers should be aware of changes in the law and technology that affect how their clients collect, store, use, obtain, and sell PII (or personal data). Lawyers should be familiar enough with the global and national changes in the law, such as those discussed above, and technology to advise their clients of red flags that they may see in their clients' businesses. For example, if an attorney finds that his or her client keeps sensitive personal information, such as SSNs, laying around the office or on a computer with no security controls (e.g., no automatic lock after a certain amount of time), that attorney should be able to recognize that this conduct contains risks that may require that client to consult with a data privacy attorney.

2. Georgia Rule 1.6, Confidentiality of Information.

Georgia Rule 1.6(a) provides:

> A lawyer shall maintain in confidence all information gained in the professional relationship with a client, including information which the client has requested to be held inviolate or the disclosure of which would be embarrassing or would

> likely be detrimental to the client, unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, or are required by these rules or other law, or by order of the court.

Additionally, Georgia Rule 1.6(c) provides that the duty of "confidentiality shall continue after the client-lawyer relationship has terminated."

Model Rule of Professional Conduct 1.6(c) contains substantially similar language. Comment 18 to Model Rule 1.6(c) explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. 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, 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. 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.

Further, Model Rule Comment 19, "Encryption," provides that:

> 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Many law firms that are covered by HIPAA have included mandatory training on the treatment of personal health information for years. However, not as many firms have implemented mandatory training for all employees and partners on cybersecurity and data privacy. To protect client personal information and confidential information protected by privileges, firms should implement mandatory cybersecurity/data privacy training at least annually. This training includes password security, limiting access to the firm's physical facilities, locking computers, sending personal information in encrypted form, and the like. Law firms also should consider whether they need an internal or external Data Protection Officer to understand and coordinate the firm's treatment of PII and ensure that adequate security measures are implemented.

Adequate security of the personal information a law firm hosts is not only required by CCPA and GDPR, but it appears to be an ethical requirement pursuant to the Rules of Professional Responsibility. Law firms should consider having a Chief Information Security Officer ("CISO") who oversees the implementation and maintenance of the firm's electronic security systems, including updates and patches as they are released. Firms should allocate sufficient funds to adequately cover implementing these measures. CISOs should work with the law firm's management regarding the practices of the firm, any new treatment of personal information and staying current with the ever-evolving laws in this area.

3. <u>Georgia Rule 4.4, Respect for Rights of Third Persons</u>.

Georgia Rule 4.4(b), Respect for Rights of Third Persons, provides:

> 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.

Comment 2 to the Georgia Rules, Metadata, elaborates on Georgia Rule 4.4(b):

> Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an e-mail or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the document or electronically stored information, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person. For purposes of this Rule, "document or electronically stored information" includes, in addition to paper documents, e-mail and other forms of electronically stored information, including embedded data (commonly referred to as "metadata"), that is subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.

Accordingly, the Rule and Commentary set out the obligations of attorneys to notify a sender of inadvertently sent electronically stored information, including metadata.

Georgia's Rule is similar to MRPC 4.4., except that Model Rule 4.4 does not appear to require the receiving lawyer promptly to notify the sender of the inadvertently sent ESI. Instead, the Model Rule appears to leave the decision to the professional judgment of the lawyer. Model Rule 4.4, Comment 3, provides as follows:

> **Comment 3 ("Deleting Information")** Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent. Where a lawyer

> is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer.

Georgia Rule 4.4 dovetails with data breach notification law. If a lawyer inadvertently sends an email or document to an unintended recipient, then this may constitute a data breach pursuant to applicable law. However, the sending lawyer may not know of the inadvertent disclosure of PII unless the receiving lawyer notifies the sender, consistent with Georgia Rule 4.4. Further, if the personal information inadvertently sent is that of a California resident, and the sending lawyer's firm otherwise meets the criteria of CCPA for it to apply, then that firm should consider notifying the California resident of the breach. Under Model Rule 4.4, however, notification of the inadvertent email containing PII appears to be optional and based on the receiving attorney's professional judgment.

4. <u>Georgia Rule 5.3, Responsibilities Regarding Nonlawyer Assistants</u>.

Georgia Rule 5.3 concerns a lawyer's responsibilities with regard to non-lawyers employed by or working with the lawyer. Generally, partners, lawyers with managerial authority and supervisors in the firm are required to make reasonable efforts to ensure that the non-lawyer's conduct is compatible with the professional obligations of the lawyer. Moreover, Rule 5.3 makes a lawyer responsible for the conduct of the non-lawyer under certain circumstances. The Rule provides:

> a. a partner, and a lawyer who individually or together with other lawyers possesses 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;
> b. a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;

c. a lawyer shall be responsible for conduct of such a person that would be a violation of the Georgia Rules of Professional Conduct if engaged in by a lawyer if:
    1. the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
    2. the lawyer is a partner in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

The comments to Georgia Rule 5.3 elaborate that lawyers are responsible for establishing policies and procedures to provide reasonable assurances that non-lawyers in their firm act consistent with the Georgia Rules of Professional Conduct, including maintaining information as confidential. Comments 1 and 2 of Georgia Rule 5.3 provide as follows:

> **Comment 1 ("Lawyers are Responsible for Everyone Else")** Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer should give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.
>
> **GA Comment 2 ("Internal Policies & Procedures")** Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that nonlawyers in the firm will act in a way compatible with the Georgia Rules of Professional Conduct.

Georgia Rule 5.3 again dovetails with data privacy laws, including CCPA and GDPR. Lawyers should ensure that the non-lawyers in their firm—employees or other assistants – understand that the personal information of clients and others that they collect, store and use should be maintained as confidential and not treated carelessly. If laptops are removed from the firm containing personal information, they should be registered and authorized with the firm, with the ability to remotely delete the contents, if lost or stolen.

Non-lawyers working with the firm, as well as lawyers, should be trained on other procedures to ensure data privacy. In addition to only using firm-approved devices, they should be trained on password security, physical security (such as not allowing "tail-gating" into the firm after swiping an access card), and email/data security. Still ranking among the highest percentage of data breaches are phishing attacks. Non-lawyers (and lawyers) should be trained on recognizing a spoofed email, not clicking on links or attachments from unknown senders, not providing user and password information in unexpected or unusual emails, and the like.

While these data security measures are not written into the Georgia Rules or the Model Rules, they are consistent with otherwise meeting the obligations of the Rules. Moreover, not taking these kind of measures could expose lawyers to complaints of violations of the Rules of Professional Conduct, in the event personal information of clients is disclosed in a data breach, as well as liability pursuant to applicable data privacy laws.