Thursday, November 4, 2021
11:00 AM – 12:15 PM

Workshop 13

Privacy and Data Security: E-Notaries, E-Closings and E-Volving state laws

Presented to

2021 U.S. Law Conference
San Francisco Marriott Marquis
San Francisco, CA
November 3-5, 2021

by:

Gary A. Kibel
Partner
Davis+Gilbert LLP
1675 Broadway
New York, NY 10019
gkibel@dglaw.com

Orlando Lucero
Vice-President/New Mexico State
Underwriting Counsel/Back-Up
State Counsel Oklahoma
FNF Family of Companies
8500 Menaul Blvd. NE, Suite A110
Albuquerque, NM 87112
Orlando.Lucero@fnf.com

Part I: eClosings and Ethical Implications

The COVID-19 pandemic revealed people's ability (and willingness) to work away from their offices, and away from each other, with less personal, physical interaction. These successes accelerated the transition to a digital office with less reliance on paper to communicate and fewer printed documents. While predictions have varied about the extent to which these effects will persist in the short term (i.e., once people return to their offices), they certainly preview what's to come.

Real estate settlements and closings are not immune to this transition. The speed with which the transition occurs, and when it will be complete, merely depends on the participants. What once required a trip to the office of a settlement attorney or title or escrow company to review a stack of closing documents to be executed in the presence of a notary public can now be done entirely on a cell phone, should that be the customer's wish.[1] The traditional hands-on paper closing and the entirely electronic closing (or "eClosing") represent the ends of the spectrum. Within that spectrum there other types of closings that comprise elements of both extremes. Whatever the exact form the closing takes, it is reasonable to assume that more and more closings will be done partially or fully via electronic means, as customers increasingly demand that level of service and convenience.[2]

What has not changed, however, are the lawyer's ethical responsibilities in representing parties to an eClosing or in conducting an eClosing. These types of closings not only implicate all of the usual ethical obligations inherent in the lawyer's role in a closing, whether that role is as a settlement attorney or an attorney representing a party to the transaction, but the electronic nature of the closing itself presents new twists on different ethical issues. While some

---

[1] This assumes remote online notarization is legally permissible in the jurisdiction where the closing occurs. See fn. 7.

[2] A 2015 report of the federal Consumer Financial Protection Bureau (CFPB) found that borrowers can benefit from electronic closings. "[T]he results of the pilot indicate that those who close their mortgage using an electronic platform are general better off on measures of understanding, efficiency, and feeling empowered than borrowers who used just paper forms." CFPB Report, August 5, 2015. https://www.consumerfinance.gov/about-us/newsroom/cfpb-study-finds-electronic-mortgage-closings-can-benefit-consumers/

of those issues can be resolved based upon existing rules, or by analogy to them, eClosings also present novel questions that will take professionals to negotiate, or rule-making bodies to work out.

What is an eClosing?

Particularly given the numerous sets of evolving eClosing procedures, parties participating in eClosings must work from the same glossary of terms to ensure a meeting of the minds and a timely closing.

Traditional Closing. A closing where all of the documents are "wet" signed, meaning that the parties and the notary physically sign the paper documents by putting pen to paper in their physical presence.

Hybrid eClosing. A closing where the parties appear in person before the person conducting the settlement and where some of the documents are wet signed and some are electronically signed or electronically notarized. An electronic signature can mean many different things but is used here to connote a "signature" that is captured in an electronic medium and which constitutes the acknowledgement or adoption of an electronic transaction or document. For example, the Uniform Electronic Transactions Act (UETA)[3] defines an electronic signature as "an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. UETA § 2(8).[4] This definition is nearly identical to that under the federal Electronic Signatures in Global and National Commerce Act (E-Sign Act),[5] which defines an electronic signature as an "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Id. The electronically signed documents should be recordable in the recording office of the jurisdiction.

eClosing. A closing where the parties appear in person before the person conducting the settlement and where all documents are electronically signed by the parties and by the notary. The electronically signed documents should be recordable in the recording office of the jurisdiction.[6]

Online eClosing. A closing where the parties and the person conducting the settlement are not in the same physical space and where all of the documents are electronically signed and electronically notarized using audio and video webcam technology. This type of closing will utilize the technologies associated with Remote Online Notarization (RON).[7] These documents too should be recordable in the recording office of the jurisdiction.

Thus, the term eClosing can be used, and is used here, to encompass both Hybrid eClosings and Online eClosings. There are numerous platforms from many different vendors available for closings that have been adopted by title companies and lenders. Some of the more well-known names include Pavaso, DocuSign, SignNow, and LegalESign. While there are obvious and necessary similarities in these platforms, there are not uniform standards among them. As a result, the proliferation of eClosing platforms has complicated the lawyer's ethical obligations when evaluating and selecting third party vendors.

---

[3] Uniform Electronic Transactions Act (UETA), Unif. Law Comm'n (1999).

[4] Forty seven states, the District of Columbia, and the U.S. Virgin Islands have adopted UETA. Section 7 of UETA gives legal recognition to electronic signatures, records and contracts. Washington, Illinois, and New York have not adopted UETA but have adopted substantially similar laws making electronic signatures enforceable. Puerto Rico is the only U.S. jurisdiction without a law like UETA.

[5] Pub. L. 106–229, title I, § 101, June 30, 2000, 114 Stat. 464, 15 U.S.C. ch. 96).

[6] Uniform Real Property Electronic Recording Act (URPERA), Unif. Law Comm'n (2005). According to the Property Records Industry Association (PRIA) as of July 31, 2019 over 3600 jurisdictions in the United States accept erecordings. According to PRIA only Kentucky and Vermont do not have any jurisdictions that accept erecordings. ALTA Title News Nov. 2019.

[7] As of June 2021 approximately thirty six states had adopted some form of RON statute. See, https://www.docverify.com/Products/E-Notaries/What-States-Allow-Electronic-Notary. Most states that have since adopted a RON law have incorporated the following key principles first established by Virginia, such as: (i) establishing what constitutes "personal appearance," for purposes of RON, (ii) how to reliably establish the signer's identity, (iii) the location of the parties, and (iv) record keeping. Because RONs are electronic records, E-Sign and UETA require that the record cannot be altered after signing and notarization with detection.

The Lawyer's Role in the eClosing

A lawyer may perform many roles in connection with an eClosing. The lawyer may be an adviser to the client, whether a seller, buyer or lender. The lawyer may be a participant in the eClosing, perhaps acting as a notary. The lawyer may be the settlement agent responsible for conducting the eClosing, whether in person or remotely, using someone else's technology or using the lawyer's own technology. While each of these roles implicates many of the same ethical rules, the focus below will be more on the lawyer conducting an eClosing – in effect a traditional closing with the overlay of modern technology in creating a "paperless" environment.

Ethical Rules Implicated in an eClosing

Several different ethical rules[8] come into play in connection with an eClosing. These rules also come into play in a traditional closing,[9] but the technological aspects of eClosings create additional issues. The intersection of eClosings and lawyers' ethical obligations is so new that little literature exists on the topic.

However, two recent ABA ethics opinions published by the Standing Committee on Ethics and Professional Responsibility: ABA Comm. on Ethics & Prof'l Responsibility Formal Opinion 477R, *Securing Communication of Protected Client Information*, (May 11, 2017, Rev. May 22, 2017),[10] and ABA Comm. on Ethics & Prof'l Responsibility Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack* (October 17, 2018)[11] elucidate ideas and principles that are useful in trying to understand a lawyer's ethical obligations in the eClosing context. Among them, the duty of competence and the duty of confidentiality as analyzed in the two formal opinions must be considered first.

The Duty of Competence

Model Rule 1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." MODEL RULES OF PROF'L CONDUCT 1.1 (Am. Bar Ass'n 2016). Recognizing "the increasing impact of technology on the practice of law and the corresponding duty of lawyers to develop an understanding of that technology,"[12] in 2012 the ABA modified Comment [8] to Rule 1.1 to read as follows:

> 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

---

[8] Because of numerous differences among state laws, these materials focus only on the ABA Model Rules of Professional Conduct. MODEL RULES OF PROF'L CONDUCT (Am. Bar Ass'n 2016). https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/? The ABA Model Rules were first adopted in 1983 by the ABA House of Delegates, and they serve as the models for the ethics rules of most jurisdictions in the United States. Some states have adopted the rules verbatim, while others have adopted substantially different versions. Since compliance with ethical rules is governed by state law or state court rules, the discussion in this paper is general guidance only and must be read in conjunction with the rules applicable in a particular jurisdiction. By way of comparison, the American Law Institute has published its Restatement (Third) of Law Governing Lawyers (2000). The Restatement has substantial overlap with the Model Rules, but it is not identical.

[9] For example, Model Rule 1.7 addresses concurrent conflicts of interest. For example, if a lawyer is conducting a real estate settlement, including the preparation of closing documents, the scope of that engagement must be made clear to the seller and buyer and the parties must give their written informed consent to the joint representation. Rule 1.7, Comment [2]. What constitutes "informed consent" is explained in detail in Rule 1.7, Comment [18]. This paper does not address ethical obligations that may exist in addition to the duties discussed herein with respect to the eClosing context. See, e.g., *Ethics Jeopardy for Real Estate Lawyers*, ACREL October 1999. https://cdn.ymaws.com/acrel.site-ym.com/resource/collection/8CD585C9-0FD8-42C5-A162-9590402FE64E/a002102.pdf. In addition, there may be state laws that address and govern the role of the real estate settlement attorney. For example, Virginia regulates settlement attorneys. *Regulations of Attorney Real Estate Settlement Agents*. Va. St. Bar, 15 VAC 5-80-10 to -50 last revised 6/26/12. https://www.vsb.org/pro-guidelines/index.php/crespa-regs/

[10] This opinion was an update to ABA Formal Opinion 99-413 *Protecting the Confidentiality of Unencrypted E-Mail* (1999).

[11] As stated in the introduction to Formal Opinion 483: '[i]n Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet. This opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach, and it addresses only data breaches that involve information relating to the representation of a client." ABA Formal Opinion 483, p. 1.

[12] Formal Opinion 477R, p. 3.

and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and

Comment . . . [8] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.[13]

Formal Opinion 483 expands the concept of lawyer technological competence, by stating:

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[14]

The Duty of Confidentiality

Model Rule 1.7 provides:

(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).
(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.

MODEL RULES OF PROF'L CONDUCT 1.7 (Am. Bar Ass'n 2016).[15]

Comment [18] as amended in 2012 provides:

[18] 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.

ABA Opinion 477R makes it clear that "[t]he Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply the core duty of confidentiality in an ever-changing technological world requires some reflection." The opinion states that "lawyers must exercise reasonable efforts when using technology in communication about client matters." Rather than imposing a "hard and fast rule," the opinion identifies various nonexclusive factors to make the "reasonable efforts" determination, including:

- the sensitivity of the information
- the likelihood of disclosure if additional safeguards are not employed

---

[13] Id.
[14] Formal Opinion 483, p. 4.
[15] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Model Rule 1.9(c)(2).

- 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)

The opinion is clear that the nature of the information being communicated, the methods of electronic communication and the types of available security measures will all come into play in determining the level of protection that is warranted.

The committee recommended the following steps lawyers should take to guard against disclosures:

1. **Understand the nature of the threat.** Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.
2. **Understand how client confidential information is transmitted and where it is stored.** Understand how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.
3. **Understand and use reasonable electronic security measures.** Understand the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.
4. **Determine how electronic communications about clients' matters should be protected.** Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications; if the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.
5. **Label client confidential information.** Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.
6. **Train lawyers and nonlawyer professionals in technology and information security.** Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.
7. **Conduct due diligence on vendors providing communication technology**. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.[16]

Formal Opinion 483 provides additional guidance with respect to confidentiality, as follows[17]:

> As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable. Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access. As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:
>
> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks,

[16] Opinion 477R, p. 6.

[17] Opinion 483 does not supplant other federal or state laws around data breaches. The opinion imposes pre breach obligations and defines data breach more broadly than other similar data breach laws.

verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[18]

Formal Opinion 483 concludes with the following:

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."[19]

The Duty to Communicate

In addition to the duties of competence and confidentiality, both Opinion 477R and Opinion 483 address the duty to communicate with the client.

Opinion 477R provides:

> Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved. The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion. A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, "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."[20]

Almost the entire subject of Opinion 483 is the duty to communicate. As explained and emphasized in the opinion:

> Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.
>
> Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach." The Committee advised:
>
> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).
>
> A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data

[18] Opinion 483, p. 9.
[19] Opinion 483, pp. 15-16.
[20] Opinion 477R, p. 11.

breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

What These Principles Mean for Lawyers in eClosings

While the rules themselves, commentary, and formal opinions have expanded our understanding of the rules in connection with specific matters dealing with practicing law in the cyberworld, none of these directly addressed the eClosing context. How do, or should, these principles apply to an eClosing?

First, clearly the duty of competence mandates that a lawyer understand the technology associated with eClosings and eClosing platforms and in particular understand and take appropriate steps to mitigate the cybersecurity risks of such platforms. Competency takes on special urgency in light of the rapid technological advances in the world of eClosings. And, the more sensitive the information involved in the closing, the greater the measures that must be taken to ensure the security of the transaction. What might comply with a lawyer's ethical obligations today and for a particular transaction might not tomorrow and for a different one. Just as adopting an old form of written agreement without considering its application to the new circumstance, an individual analysis of the transaction is required to ensure the platform and measures used to protect the transaction are adequate, particularly as technology and business practices and protocols constantly change. Perhaps the most frightening, and likely, aspect of all of this is that a lawyer may not even know what he or she doesn't know.

Second, the duty of confidentiality has to guide everything a lawyer does in conducting eClosings. A lawyer should anticipate having to comply with the highest level of "reasonable efforts" to protect the identity of the clients, client information and the security integrity of the transaction. Of course, what is reasonable in one transaction might be overkill or totally inadequate in another. The prudent lawyer will heed the admonitions of Opinion 477R[21] and understand the following seven factors in the context of an eClosing and implement appropriate measures.

1. **Understand the nature of the threat.** The nature of client information transmitted in an eClosing is highly sensitive and may include items of personally identifying information (SSN, birthdate) and financial information (bank accounts, securities accounts, credit card accounts), all of which is a treasure trove to a hacker seeking to steal someone's identity. The risk associated with a hack of this information suggests that greater protection may be warranted, whether the lawyer is using his or her own eClosing platform, advising a client using a lender's eClosing platform, or conducting the eClosing with a third-party platform.

2. **Understand how client confidential information is transmitted and where it is stored.** Compliance with this factor involves not only having a basic understanding of how the eClosing platform gathers, manages and accesses client data, but also how the lawyer's computer systems communicate and integrate with that platform. The lawyer needs to evaluate for security compliance any device that may be used with the eClosing platform and implement appropriate security measures. Just because the laptop in the lawyer's office may be sufficiently secure, the lawyer's cell phone may not be.

3. **Understand and use reasonable electronic security measures.** The lawyer needs to understand the array of security measures that are available to provide reasonable protections for client data. Given the highly sensitive nature of information involved in an eClosing, reasonable security efforts may require the highest level of security measures, such as multi-factor authentication (via text to known device) or knowledge-based authentication. Does the platform

[21] Opinion 477R, p. 6.

provide for signed document lock with tamper evident markers? Does the platform provide secure storage and retrieval of an electronically signed document? And for how long

4. **Determine how electronic communications about clients' matters should be protected.** In the eClosing context, the lawyer may be communicating with the client or clients as well as the lender or other parties. The lawyer has the obligation to discuss with the client the level of security that is appropriate for the transaction, and the lawyer has to coordinate or otherwise try to ensure that the entire transaction is conducted with the appropriate level of security. This factor also addresses the sophistication of the client. For example, if the client is unsophisticated or has limited access to appropriate technology protections, it may be the lawyer's obligation to advise the client not to undertake an eClosing or to try to ensure a secure environment in which the client may participate in the eClosing, e.g., using a law firm computer at the law office instead of the client's old unsecure one.

5. **Label client confidential information.** It is unclear how this factor would be put into practice in an eClosing. Certainly, if the lawyer is representing a client in the transaction, all communications between the lawyer and the client should be labeled as confidential. To the extent that the lawyer is sharing client information on the eClosing platform, the lawyer should mark that information as confidential, assuming that would be permitted by the platform technology. If the lawyer is conducting the settlement for all parties via an eClosing platform, the entire transaction would have to be marked as confidential within the platform, if possible.[22]

6. **Train lawyers and nonlawyer assistants in technology and information security.** The lawyer will be responsible for making sure that everyone else in the firm working on eClosings understands all of the technologies and their obligations to comply with the factors discussed here. Understanding the rapid nature of technological change will further require constant monitoring and reassessment of the security elements of the eClosing platforms. The need to stay abreast of technological advances may, for example, mean limiting the number of eClosing platforms utilized; if the lawyer is using too many different platforms it may become impossible to stay up to date (i.e., competent).

7. **Conduct due diligence on vendors providing communication technology**. eClosings bring this factor into stark relief. Most individual lawyers are unlikely to have all of the information and tools necessary to understand and evaluate the cybersecurity features of an eClosing platform. By necessity most lawyers will need to rely on third parties, whether persons inside of the law firm or other third parties to undertake the required due diligence. For purposes of selecting an eClosing platform, the lawyer has an obligation to communicate with the vendor and take appropriate steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer. Issues for the lawyer working with a third-party vendor on an eClosing platform for use by the closing lawyer might include the following, depending on the circumstances. [23]

- Ensure that the service provider and technology they use support the lawyer's professional obligations. Incorporate those obligations and an acknowledgement of understanding them into the contract, if possible.
- Understand the service provider's terms of service, service level agreement, privacy policy and security policy. Does the contract adequately address concerns regarding protecting clients' rights and allowing the lawyer to fulfill professional obligations? Does the contract ensure that the confidentiality and privilege of their clients' information is protected? Are there meaningful remedies for breach?
- Try to ascertain where the data is stored/hosted.
- Confirm who owns the data. Confidentiality and privilege are rights held by the client. Lawyers must ensure ownership of their clients' information does not pass to the service provider or a third party.
- What happens if the service provider goes out of business or has their servers seized or destroyed? What if the service provider is hacked? Does the service provider have the obligation to notify the lawyer, in addition to the client? How quickly? What information is required to be provided?
- How easily can the lawyer migrate data to another provider or back to desktop applications?
- Who has access to the data and for what purposes?

---

[22] For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Model Rule 5.3, Comments [3]-[4].

[23] This list is based in part on this excellent checklist: The Law Society of British Columbia, *Cloud computing checklist v. 2.0* (updated May 2017), https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/checklist-cloud.pdf

- Does the service provider archive data for the retention lifecycle the lawyer requires? For example, many platforms retain the electronic documents for only a few months.
- Are there mechanisms to ensure data that is to be destroyed has been destroyed? Are certifications of destruction adequate or acceptable?
- What are the lawyer's remedies for the service provider's non-compliance with the terms of service, service level agreement, privacy policy or security policy?
- What is the service provider's reputation? Is this a vendor to whom a lawyer should entrust client information?
- Does the service provider sell its customer information or otherwise try and commoditize the data stored on its servers?
- What security measures does the service provider use to protect data, and is there a means to audit the effectiveness of these measures?
- Lawyers should establish a record management system, and document their decisions with respect to choosing an eClosing platform.

One issue to note briefly is the security of the flow of money in any closing, whether a traditional closing or an eClosing. A lawyer's handling the escrow of monies in a closing must have sufficient security protocols in place to try to avoid being hacked and sending money to the wrong party.[24] For example, in the title insurance world, title companies will not accept email changes to wiring instructions without some further communication, usually by telephone, with the intended recipient of the wired funds. Dual controls and segregation of duties is probably appropriate (i.e., person initiating wire transfer is different from person approving it). Preventing wire fraud requires ongoing training of all persons involved in the chain of a wire transfer and constant vigilance.

Lastly, as Opinion 483 makes abundantly clear, in the event of a data breach that includes client information, whether within the law firm itself or within the eClosing platform, the lawyer has a variety of notification obligations. On the front end, the lawyer has to try to make sure that the lawyer is notified of any data breaches within the eClosing platform so that the lawyer may comply with his or her ethical obligations to inform the client. On the back end, as soon as the lawyer is informed of a data breach from the eClosing platform provider, the lawyer should undertake the notifications described in Opinion 483.

Conclusion

eClosings pose great promise and great risk. eClosings represent the future of many, if not most real estate transactions. A lawyer's essential role in the closing process, whether as counselor or as closer, will not change, but the means by which the lawyer fulfills those roles will most definitely change. The well-prepared lawyer will be ready to meet the challenges of eClosings and comply with his or her ethical obligations. The future is here – let us embrace it!

Part II: Privacy and data security: E-volving state laws

Apple Makes Big Changes to Its Tracking System

With the launch of iOS 14.5 slated for next week, Apple's long-awaited changes to the use of its persistent identifier known as the "Identifier for Advertisers" (IDFA) have now gone into effect. While this change has been explained by Apple as a step to protect its users' privacy, it will drastically change the ability of third parties and app publishers to collect information on and track users through apps on Apple devices.

Apple's Changes to IDFA

As of the launch, app publishers on Apple's iOS 14.5 platform have to receive a user's permission through Apple's new "AppTrackingTransparency" framework at the app level in order to track a user or access a user's IDFA for purposes of targeted advertising or advertising measurement.

This means that when using an app, Apple users will be presented with a one-time notification that will explain how their IDFA will be used for tracking, and will then give the users the choice to either opt-in or block the sharing of the IDFA at the app level (an option which was previously available to users only as an opt-out option located in a user's Apple Settings).

---

[24]Pennsylvania law firm had to bear loss of $580,000- wired to hacker who had compromised law firm shareholder's email.
http://www.mondaq.com/unitedstates/x/798776/Security/Hacked+Law+Firms+Left+Holding+The+Bag

Experts believe that this change will significantly reduce the percentage of Apple app users who share their IDFA with the app publishers, presenting a big challenge for the marketing efforts of these publishers and the ad tech companies with who they work.

While Apple's policies and terms are not laws, in many ways they have a greater impact than some new privacy laws given how critical use of the Apple platform is to many businesses. Therefore, compliance cannot be overlooked, since a failure to comply could result in Apple taking corrective measures against an app publisher.

Apple's changes to IDFA come on the heels of the announcement from Google in 2020 that they would be blocking the use of third-party cookie technology in the Chrome browser, a technology widely used in the ad tech industry for retargeting. Google has proposed cookieless alternatives via proposals in its "privacy sandbox." The most prominent is call FLoC (Federated Learning of Cohorts), which relies upon aggregating browser activity into cohorts with similar online habits. Interestingly, Google recently announced that they would not be testing FLoC in the EU, which has stricter privacy regulations than in the U.S.

The Ad Tech Industry Responds

The announcements from Apple and Google will require significant changes to the way that advertisers track and retarget users. Advertisers will have fewer authenticated users to target with ads across the various platforms. As a result, advertisers are looking for new and creative ways to adapt in the changing privacy landscape. One solution is the "Unified ID 2.0", a collaborative industry approach, which proposes a universal, anonymized user identifier that would require a user to opt-in once across all digital channels and devices to receive applicable ads. The proposed Unified ID 2.0 would offer protection to consumers, since the identifier would be a hashed and encrypted version of the user's email address, while also providing advertisers with a targeting and tracking alternative to third party cookies. There are numerous private proposals for new pseudonymous IDs listed as open source on the website prebid.org.

The Interactive Advertising Bureau (IAB) has also introduced its own initiative, Project Rearc, to address the loss of third party cookies on these large platforms. In March of this year, Project Rearc released for comment new proposed standards and guidelines for how companies should collect and use consumer identifiers in this new environment. Many advertising trade associations have joined forces to establish a new group, the Partnership for Responsible Addressable Media or "PRAM." PRAM is actively working on standards and principles for new forms of addressable media that enable businesses to connect with consumers in a privacy-friendly manner in compliance with applicable laws and platform rules.

The Bottom Line

- Apple's changes to IDFA and Google's announcement blocking third-party cookies in Chrome will change advertisers' ability to track and retarget users as they have in the past.
- All participants in the online advertising ecosystem, including publishers, ad tech companies and advertisers, should consider these developments and how best to execute effective campaigns in this new reality.

Virginia Becomes the Second State to Pass a Comprehensive Privacy Law

After passing with relative ease through Virginia's House of Delegates and Senate, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA) into law on March 2, 2021. Virginia joins California as the only states in the nation to have passed comprehensive privacy legislation. Companies that are subject to the new law will have to comply beginning January 1, 2023, the date when the law goes into effect. Companies should note that this date coincides with the effective date of the new substantive obligations set forth in the California Privacy Rights Act (CPRA), the recently passed ballot initiative amending the California Consumer Privacy Act (CCPA), as discussed in our previous alert.

While the new Virginia law creates a hybrid model that borrows liberally from the CCPA and CPRA, as well as the EU's General Data Protection Regulation (GDPR), it also contains many unique elements that diverge from these counterparts.

Details of the CDPA

The threshold question for companies to consider will be whether the new law applies to their specific organization. The CDPA will apply to persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that controls or processes personal data of at least:

- 100,000 “consumers” during a calendar year; or
- 25,000 “consumers” and derives over 50 percent of gross revenue from the “sale” of personal data.

Consumer
It’s important to understand that “consumer” only includes Virginia residents that are acting in an individual or household context and specifically excludes persons acting in a commercial or employment context. Accordingly, businesses do not need to consider data collected from its employees or from business contacts as personal data under the CDPA.

Sale of Personal Data
Businesses will need to consider whether they “sell” personal data under the law. Unlike its California counterpart, the “sale” of personal data is narrowly defined as “the exchange of personal data for monetary consideration by the controller to a third party.” In other words, monetary consideration must be paid to the business in order for a “sale” to occur. The CDPA also specifically excludes, among other things, disclosures to a business’ affiliate from the definition of a “sale”.

Personal Data
As with any privacy law, the definition of personal data is critical to assessing the scope of the law. The CDPA simply defines “personal data” as information that is linked or reasonably linkable to an identified or identifiable natural person. It specifically excludes de-identified data and publicly available information. The definition does not reference information that is linkable to a household, as is the case in the CCPA/CPRA.

Sensitive Data
Like the CPRA, the CDPA defines “sensitive data” to include personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, as well as genetic or biometric data used for the purpose of uniquely identifying a natural person, the personal data collected from a known child, and precise geolocation data. Notably, a business will need to obtain a consumer’s consent before it can process sensitive data.

Consumer Rights
The CDPA makes available certain core rights to consumers (similar to those found in the GDPR). In fact, the new law uses the terms “controller” and “processor” which are the same terms used under GDPR, although the definitions are not identical.

In particular, the CDPA gives Virginia consumers the right to:

- Confirm whether or not a controller is processing the consumer’s personal data and to access such data;
- Correct inaccuracies in their personal data;
- Delete their personal data;
- Obtain a copy of personal data that the consumer provided to the controller in a portable and, to the extent technically feasible, readily usable format; and
- Opt-out of certain types of processing, including the sale of personal data, as well as the use of personal data for purposes of “targeted advertising.”

Data Controller Responsibilities

Limitations on Processing
Similar to the GDPR processing principles, the CDPA incorporates certain limits on processing that generally apply to the controller of personal data, which include obligations to:

- Limit the collection of personal data to what is “adequate, relevant and reasonably necessary” in relation to the purpose for which the data was collected;
- Implement and maintain reasonable security practices to protect personal data;
- Restrict the use of personal data for new purposes that are incompatible with the purposes for which it was collected;
- Not discriminate against consumers for exercising their consumer rights; and
- Obtain consent before processing any sensitive data.

Privacy Policy
Controllers are required to provide consumers with a privacy policy that is reasonably accessible and includes:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers can exercise their rights (and appeal a controller's decision with regard to the consumer's requests);
- The categories of personal data shared with third parties; and
- The categories of third parties with whom personal data is shared.

Transparency Regarding Sales and Targeted Advertising
If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing as well as the manner in which a consumer can opt-out. Notably, there is no mandate as to how these disclosures must be made.

Data Processing Agreements
Similar to the GDPR, the CDPA requires a contract to govern a processor's data processing procedures performed on behalf of the controller. The contract will need to set forth the instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. Certain mandatory requirements must also be imposed on the processor, including requirements to make available all information to demonstrate the processor's compliance with the CDPA, submit to assessments conducted by the controller (or, alternatively, have an independent assessment conducted), and to flow down the processor's obligations on any subcontractors engaged by the processor.

Data Protection Assessments
The CDPA also requires the controller to conduct data protection assessments of the risks associated with certain enumerated processing activities, including the processing of personal data for targeted advertising, the sale of personal data, the processing of personal data for profiling (if such profiling presents certain risks of harm to consumers), the processing of sensitive data, and other processing that presents a heightened risk of harm to consumers. The law does not specify how often such assessments must be conducted.

Enforcement; No Private Right Of Action
Enforcement of the CDPA will be the responsibility of the state attorney general. There is no private right of action. Notably, the CDPA contains a 30-day notice period that allows a controller to cure violations that have been brought to its attention by the attorney general. This contrasts with the CPRA which will remove a similar cure period that is currently included in the CCPA. Violations that have not been cured within 30 days are subject to a fine of up to $7,500 per violation.

The Bottom Line

- While Virginia is now the second state with a comprehensive consumer privacy law, it certainly will not be the last.
- With CCPA already in effect and the CDPA and CPRA both on the horizon, companies will need to begin planning now to update their privacy programs to ensure compliance with these conflicting standards.

Don't *Smile at the Camera — New Biometric Data Laws*
Biometric data is seen as a preferred means of identification by many businesses. Unlocking a smartphone using facial recognition and other biometric identifiers, for example, gives users the feeling as if they are more protected (e.g., less risk of identity theft). However, similar to the boom in privacy developments and legislation related to the collection and use of more traditional personal information, the growth of biometric data use by businesses, law enforcement, employers and other organizations has given rise to renewed privacy concerns and legal developments.

While there is no uniform federal biometric data privacy law, several states either have existing laws or are in the process of drafting or ratifying new laws. Although it remains to be seen how such legislation will change the industry's use of and reliance upon biometric data, that it is increasingly the subject of analysis and discussion indicates a demand and a need for reasonable security and privacy practices around the collection and processing of biometric data, whether required by law or not.

Existing State Laws — Illinois
While several states, including Texas, Washington, California, New York and Arkansas have existing laws that directly govern or otherwise address biometric data in some fashion, only one, Illinois, has a comprehensive law

that offers a private right of action to aggrieved individuals. The Illinois Biometric Information Privacy Act (BIPA) imposes rigorous requirements on businesses that collect or otherwise process biometric data, including, requiring consent from the consumer before the collection, and disclosure of their policies regarding use and retention, of such data.

Unique to BIPA is the individual's private right of action, whether actually injured or not by the BIPA violation. In Rosenbach v. Six Flags Entertainment Corp., the Illinois Supreme Court held that a violation of BIPA alone, regardless of damage or injury, is enough to give rise to such private right of action. If found to be in violation of BIPA, penalties (on a per-violation basis) may range from $1,000 to $5,000. As a result, BIPA has become a favorite tool of class action lawyers and an expensive issue for businesses.

New and Pending State Laws — Oregon & New York

The City of Portland, Oregon, enacted a city-wide ordinance on January 1, 2021 prohibiting (with a few exceptions, e.g., for compliance with law and user verification purposes) the use of facial-recognition technology by private entities in places of public accommodation (which are defined as, "any place or service offering to the public accommodations, advantages, facilities or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise.").

Notably, in addition to standard privacy concerns, the genesis of this statute seems to have derived from a concern that all residents and visitors of the city be treated fairly and equally with respect to surveillance and the use of biometric data, as well as growing evidence that some uses of facial recognition technologies have resulted in misidentification and biased practices with respect to race and gender.

There is some uncertainty around what constitutes "facial-recognition technology," as well as whether informed consent creates an exception to the prohibition since the ordinance does not address how an individual's consent to the collection and use of such data would impact the prohibitions. Similar to BIPA, the Portland ordinance also provides for a private right of action, with penalties up to $1,000 per day for each day of the violation.

On January 7, the New York State Legislature proposed the Biometric Privacy Act (BPA). Whereas the Portland ordinance prohibits outright the use by private entities of facial recognition technologies, the BPA seeks instead to enhance the privacy rights of individuals and controls around the collection and processing by private entities of biometric information.

Prior to collection, the individual must be informed of the:

- Specific biometric data to be collected,
- Purpose and duration of the collection and use, and
- Individual must give written consent to the foregoing.

Additionally, the BPA imposes restrictions on the use and disclosure of such biometric data by the entity that collected or otherwise received it. The BPA also provides "aggrieved" individuals with a private right of action with penalties ranging from $1,000 to $5,000 (or, if greater, actual damages).

The Bottom Line

The confluence of privacy, security, societal and other reasons have resulted in increased scrutiny over the use of biometric data through new proposed laws. In the absence of a consistent federal standard, businesses should assess their biometric data collection and use practices and technologies, implement a written policy, plan for the collection and use of such data, and ensure disclosures and consents, as appropriate, are given to and received by individuals whose data is collected.

Digital Media, Technology & Privacy Alert >> And the Winner of This Year's Election Is… the California Privacy Rights Act
November 5, 2020

Authors: Richard Eisert and Gary Kibel

While the 2020 United States presidential election took center stage, California voters approved the California Privacy Rights Act (CPRA) ballot measure. The CPRA makes significant changes to the existing California Consumer Privacy Act (CCPA), the landmark state privacy law that went into effect on January 1, 2020. This means that many businesses will have to revisit their CCPA compliance programs (again). For those who have yet to develop a privacy compliance program, now is an opportune time to put one in place while considering the new changes that are on the horizon.

Although most of the CPRA becomes operative on January 1, 2023, it's important to understand that the CPRA will apply to personal information collected by a business starting on January 1, 2022. While the industry has lobbied hard to amend the CCPA, the CPRA will be much harder to revise since it is a ballot initiative passed by the voters. In addition, there are a handful of provisions that will become effective five days after the California Secretary of State has certified the election results, which is expected in early December. Notable among these changes are:

- An extension of the CCPA's temporary exemptions that apply to certain business-to-business (B2B) and employment related personal information until January 1, 2023. This overrides a shorter extension that passed earlier this year, as discussed in our recent alert;
- The establishment of $10 million in funding for the "California Privacy Protection Agency," a new agency that will have full authority to implement and enforce the CCPA, and will be responsible for adopting new regulations pursuant to the CPRA. The new agency will be governed by a five-member board that must be appointed within 90 days of the effective date of the CPRA; and
- Substantially expanded instructions to the Attorney General and the California Privacy Protection Agency to adopt new regulations. The new agency will be required to begin rulemaking activity as of the later of July 1, 2021 or six months after the new agency provides notice to the Attorney General that it is prepared to do so.

In addition, businesses should take a closer look at key CPRA changes that will become effective in the (not so distant) future. Keep in mind that the CCPA already requires updates to a privacy policy every 12 months.

- **"Business" Thresholds**: The key threshold that triggered the CCPA for many companies was the purchase, receipt, sale or sharing of the personal information of 50,000 or more consumers, households or devices. For many, just the existence of a website was enough to meet this threshold given the expansive definition of personal information included data elements such as cookie IDs, IP address and device identifiers. The CPRA modifies this threshold by limiting its application to the purchase, sale or sharing (but not the receipt) of personal information of 100,000 or more consumers or households (excluding devices).
- **Sensitive Personal Information**: The CPRA adds a new definition for "sensitive personal information" which is a subset of personal information and includes government identifiers; account and login information; precise geolocation data; race; ethnicity; religion; genetic data; union membership; contents of private communications; and information concerning a consumer's sex life, sexual orientation, health and biometric information. Businesses who collect or process sensitive personal information, which specifically includes precise location data, will have to comply with new transparency requirements and offer consumers the ability to limit the use and disclosure of such data through a new link on the business' webpage, titled "Limit the Use of My Sensitive Personal Information".
- **Cross-Context Behavioral Advertising**: The CPRA amends the CCPA to explicitly address "cross-context behavioral advertising" which is defined as "the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications or services, other than the business, distinctly-branded website, application or service with which the consumer intentionally Interacts." Significantly, the CPRA treats the "sharing" of any personal information for the purpose of cross-context behavioral advertising in the same way as a "sale" of personal information under the CCPA. Among other things, this means that businesses will need to make specific disclosures and offer certain rights with respect to personal information that has been "shared" for cross-context behavioral advertising. For example, this includes the right to opt out of such sharing through a link available on the business' webpage, titled "Do Not Sell or Share My Personal Information."
- **Advertising and Marketing**: The CPRA introduces a new "business purpose" which allows service providers and contractors to process personal information to provide "advertising and marketing" services, but specifically excludes use for cross-context behavioral advertising (discussed above). This appears to

prevent any entity processing personal information for cross-context behavioral advertising purposes from being a "service provider" or "contractor" and the disclosure of personal information for such purposes will be subject to the opt-out rights discussed above. Taken together, the introduction of the "cross-context behavioral advertising" and "advertising and marketing" concepts appear to be an attempt to ensure that businesses must offer California residents the right to opt-out of cross-context behavioral advertising, regardless of any industry attempts to limit the application of such rights.

- **Publicly Available Information**: The carve-out of "publicly available" information from the definition of personal information was narrowly defined under the CCPA and only included information lawfully made available from government records. The CPRA expands this carve out to include information that a business reasonably believes is lawfully made available to the general public by the consumer or from widely distributed media. Ostensibly, this would appear to provide considerable relief for companies that primarily process personal information that has been publicly posted by the consumer through social media and similar channels.
- **Right to Correction**: In addition to the consumer rights discussed above (in relation to sensitive personal information and cross-context behavioral advertising), the CPRA also establishes a new consumer right to correct inaccurate personal information in a manner similar to that set forth in the EU's General Data Protection Regulation (GDPR).
- **General Duties**: In a nod towards Europe's GDPR processing principles, the CPRA introduces certain key "general duties" that apply to businesses. These include, among other things, an obligation to use reasonable security procedures and practices to protect personal information, restrictions against using personal information for new purposes that are incompatible with the specified purpose for which it was collected and limitations on the retention of personal information for longer than is reasonably necessary for a disclosed purpose.
- **Contracts**: While the CCPA incentivized businesses to enter into certain agreements when sharing personal information, the CPRA now explicitly requires such agreements. Certain provisions are required to be included in these agreements and are clearly aimed at ensuring that the business has obtained assurances that the personal information will be adequately protected. Similarly, service providers and contractors are required to flow down certain mandatory provisions to any persons that they engage (or that those persons may engage) to assist with the processing of personal information on behalf of the business.
- **Increased Fines / No Cure Period**: Under the CPRA, the $7,500 maximum fine for a privacy violation will also apply to violations involving the personal information of minors under 16. Currently, only intentional violations are subject to the maximum fine. All other violations will remain subject to a fine of up to $2,500 for each violation. The CCPA's 30 day cure period for violations has also been eliminated.
- **Private Right of Action**: Although the CPRA largely retains the limited private right of action that consumers can bring in connection with a security breach, the scope of the private right of action has been expanded to include breaches exposing a consumer's email address in combination with a password or security question and answer that would permit access to the account.

THE BOTTOM LINE

Now that California voters have approved the CPRA, also known as "CCPA 2.0", businesses should review (or create) their privacy programs to ensure compliance with the CCPA (in its current form, including the recently finalized regulations) as well the new changes that will take effect under the CPRA.