Your Title and Settlement Business in the Age of Privacy

Privacy laws are designed to prohibit disclosure or misuse of personal information, and some of these laws create an additional burden on title and settlement providers who receive, process, and share consumer's personal information to provide their core services. Technology and process changes can be used to mitigate this burden, while remaining compliant.

– Gorkem Kuterdem, Senior Vice President, Strategy, Adeptive Software

Privacy and Its Applicability to Title and Settlement Services

The concept of privacy, the right of an individual to protect information about themselves from unpermitted disclosure, is a touchstone of our digital and physical lives. In the last 15 years, the advent of online platforms that offer free or lower-cost services in exchange for personal information has provided a bargain that many individuals have found impossible to resist: Exchange private information for goods and services. Most of the time, this exchange is irreversible: You may be able to restrict further erosion of your privacy by declining to share more information, but it is challenging to stop the use of the private information you have already shared.

The use and abuse of consumers' private information have led to many jurisdictions implementing strict laws and regulations regarding the collection, use, sharing, selling, and retention of consumers' private information. The best known recent examples are the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act of 2018 (CCPA).

In the financial services sphere, the sharing of private information with service providers is not usually a choice, but a necessity. To ensure that information thus shared is protected, Congress enacted the

Gramm-Leach-Bliley Act (GLBA) in 1999, which required the Federal Trade Commission (FTC) to implement regulations to enforce the Privacy of Consumer Financial Information Rule ("Privacy Rule"). According to the Privacy Rule, providers of real estate settlement services are covered by the Rule and are responsible for protecting a consumer's nonpublic personal information (NPI). Per FTC's guidance, NPI is:

- any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- any information you get about an individual in connection with providing a financial product or service (for example, information from court records or a consumer report).[1]

Information deemed "publicly available" is excluded from the Rule. For example, a seller's name and property address could be "publicly available" as that information is generally accessible via public records. However, a buyer's name and the address of the property they are buying will be considered NPI.

The requirements for the safeguarding of the information are only a portion of the Rule. The Rule requires a privacy notice be provided to consumers and also provided with opt-out options regarding the sharing of their information. Except in certain circumstances, consumers must always have a "reasonable means" to opt-out of their private information being shared.

In March 2020, Senator Moran introduced the "Consumer Data Privacy and Security Act of 2020" (CDPSA), in an effort to create a preemptive and overarching data privacy framework at the federal level. It benefits from the lessons learned from the CCPA (below) while trying to combine the tenets of CCPA and GDPR. It assigns the enforcement of the Act to the Federal Trade Commission (FTC).

It carves out exemptions for "small businesses" (fewer than 500 employees and gross receipts of less than 50 million dollars over three years for the most recent six month period, and those collect or process less than 1 million individuals' personal information or the sensitive personal data of fewer than 100,000 individuals in a year).

It also aims to lessen the compliance burden of the covered entities by creating a list of "permissible purposes" that require no explicit consent from an individual and are of limited retention duration.

[1] https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

It presumes that implicit consent is present for the following specific purposes, the last of which can be further expanded by the FTC:

1. Provision of a Service or Performance of a Contract
2. Compliance with Laws
3. Immediate Danger
4. Fraud Prevention
5. Research
6. Operational Purposes

State-Level Legislative Activity

Currently, there does not seem to be any interest in passing a federal privacy law similar to the GDPR, the CDPRA notwithstanding.

At the state level, there's been a surge of activity in the legislative arena. As of this writing, there were 94 bills in state legislatures pertaining to data privacy of individuals (source: FiscalNote and ALTA). These laws, proposed or enacted, aim to strengthen the consumer rights to know what private information is collected, how and where it is stored, with whom it is shared, or to whom it is sold. There is also at least one example (CCPA) of a law that enables the consumer to request not just the disclosure, but the deletion of all collected private information about them, subject to not yet litigated constraints, such as complying with a legal obligation.

At the state level, there's been a surge of activity… to strengthen the consumer rights to what private information is collected, stored, shared, or sold.

CCPA is probably the best known of these state-level efforts, having been first proposed as a citizen's initiative, which was dropped in exchange for legislation passed by the California State Legislature and signed into law by the Governor in 2018. Its effective date is January 1, 2020; however, California consumers may be able to request information from companies subject to the CCPA on data collected for the year of 2019 due to the 12-month lookback period. As it stands today, enforcement of the law starts no earlier than July 1, 2020, but actual timelines are subject to the regulations being finalized and becoming effective.

On March 11, 2020, a second set of modifications to the proposed regulations to implement CCPA was opened for public comments, after an initial round of modifications in February 2020. The changes include:

1. A two-step opt-in process for consenting to the sale of personal information;
2. Exemptions from having to search for categories of personal information if the information meets these criteria:
    a. The business does not maintain the personal information in a searchable or reasonably accessible format;
    b. The business maintains the personal information solely for legal or compliance purposes;
    c. The business does not sell the personal information and does not use it for any commercial purpose; and
    d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
3. A requirement for the business to disclose that they collect biometric information, but not deliver it;
4. If the requested information is stored on an archival system, the business need not deliver the information stored on those systems to the consumer until the information is moved to an active system, or accessed for sale, disclosure or commercial purpose;
5. The ability for a service provider to use and retain personal information to improve internal services.
6. If a business collects more than 10 million consumers' data in a calendar year, a requirement to compile and report its compliance with CCPA to the public at large;
7. Addition and clarification of identity verification requirements for non-accountholders;
8. Addition of the possibility of the business offering a financial incentive to those consumers who opt-in to the sale of their data, in line with the value of their data.

Nevada passed its own more limited version of the "online privacy" law in 2019, as SB 220. Contrary to the CCPA, SB 220 exempts institutions covered under the GLBA and hence is likely to have minimal effect on title and settlement providers. Its crucial difference from the CCPA is that SB 220's exclusion is at the institution level, while CCPA's is based only on the context in which the private information is collected.

Texas has also passed HB 4390 in 2019, that strengthens data breach notification requirements, and sets up the Texas Privacy Protection Advisory Council to advise the Texas governor and legislature on how to address consumer privacy. The Council will deliver its findings and recommendations by Sept. 1, 2020.

A new initiative is in California to increase data privacy rights for California residents, and other states are expected to increase their activity in the privacy realm.

In light of this trend, it would be prudent to design your operational and compliance strategy by considering the current most stringent privacy law. Examining the requirements of CCPA will provide a good guideline for what to expect in the future. As CCPA's definition of private information is broader than that of the GLBA, it would be prudent to design your privacy strategy with CCPA in focus, while ensuring you are still in compliance with the GLBA Privacy Rule.

Conducting Business the CCPA Way

CCPA applies to a business located outside of California if you collect consumers' private information while doing business in California. (e.g., if you close real estate transactions where the buyer or seller is in the state of California), and:

- Are a for-profit entity that either has annual gross revenues of greater than 25 million dollars; OR
- buy, receive, sell, or share the private information of more than 50,000 consumers or households every year.

Please note that a consumer, as defined by the CCPA, is a natural person who is a California resident, and they need not have done any business with you previously.

If you control or are controlled by another entity that has the same branding as you, this test also includes their activities and revenues. The data collected under the GLBA is excluded from CCPA if the GLBA covers the data.

While the law may have originally been intended to apply to the online platform operators that collect, mine, and sell consumers' private information, it is likely that many title and settlement service providers will also be subject to the law due to having customers in California and either having sufficient revenue or transaction volume.

The definition of what constitutes private information under the CCPA is quite broad. While it excludes certain categories of information ("publicly available information," "de-identified or aggregated information," "business contact information"), it includes many data points you may not immediately think of as being covered. For example, IP addresses of devices used to access your services or the location data of your consumers are included in this definition under the CCPA.

Another issue to consider is that the same information type might be subject to the GLBA or CCPA, depending on the context in which it was collected. For example, an IP address to validate the consumer's device as part of device fingerprinting during an e-closing may be covered by the GLBA, but the same IP

address collected through your public website if the consumer visited the website to learn about you might be subject to the CCPA, for the latter is not covered by the GLBA.

The most onerous compliance aspects of the CCPA come into play if you "sell" the private information of consumers. The definition of "sale" in the CCPA is anchored by "monetary or other valuable consideration" received by the seller, but the terms are not clearly defined. In the usual course of the title and settlement processing, we regularly share consumers' private information with other parties in the transaction, including our vendors.

This sharing is not considered a "sale" as long as the parties with whom the information is shared are considered "service providers[2]," and these service providers themselves do not sell the information. Consider the need for a written agreement with your service providers outlining the specific uses for consumers' private information, its handling, and the consumers' rights under CCPA. What actually constitutes a sale will probably be the subject of upcoming litigation or clarification by the California State Assembly.

Under CCPA, companies must:

- Implement a way for the consumer to know and understand its data practices, such as the categories of private information you collected, the sources from which this information is obtained, and the categories of third parties with whom the information is shared or to whom it is sold;
- Inform a consumer about their rights under CCPA vis-a-vis the company's business practices; and
- Provide them with contact information to place an opt-out request from the selling of their information. Furthermore, employees will need training on how to process these opt-out requests.

The definition of "sale" in the CCPA is anchored by "monetary or other valuable consideration" being received by the seller, but the terms are not clearly defined. In the usual course of the title and settlement processing, we regularly share consumers' private information with other parties in the transaction, including our own vendors. This sharing is not considered a "sale" as long as the parties with whom the information is shared are considered "service providers," and these service providers themselves do not sell the information.

[2] "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing personal information for a commercial purpose other than providing the services specified in the contract with the business. (excerpted from the full text of the CCPA)

Last but not least, companies need to **provide at least two ways** to receive a "verifiable request" from a consumer and exercising their right to know which private information of theirs was obtained, processed, shared, or sold within the preceding 12 months or requesting to delete their information. The response needs to be delivered within 45 days of the request. As the law effective date is January 1, 2020, responses may need to include 2019 data.

CCPA also enables a private right of action for any consumer whose private information was subject to a data breach, if the data were not encrypted or redacted. The awardable damages include actual or statutory damages of $100-$750 per consumer per incident, whichever is greater. When the stakes for a data breach are this high, it is of utmost importance to review how customers' private information is stored and processed and to ensure a robust information security practice is in place, including a response plan in the event of a data breach event.

The awardable damages include actual or statutory damages of $100-$750 per consumer per incident, whichever is greater.

The Real Estate Transaction Ecosystem and Privacy

Title and settlement service providers regularly receive instructions from other parties that are part of the transaction, and compliance with these instructions is a critical component of the settlement process. Since the introduction of privacy laws, a number of lending institutions that are part of the real estate ecosystem have started communicating their requirements. These include how their consumers' information should be handled, retained, and removed from your systems, including settlement processing systems, emails, and even paper files.

As many of these institutions originate loans in multiple states and do not want to manage differing privacy policies by state, they are choosing to comply with the most stringent one currently known, the CCPA.

As much of the private information shared by a lender with your business is covered under the GLBA (and hence not by the CCPA), you may think that the CCPA is not a source of an additional compliance burden. However, we are aware of requests from lenders to remove drivers' license images from closing packages, redact information from documents, or delete them altogether from systems after closing. Since it is unlikely the industry will coalesce around a common set of instructions and practices soon, it is in your best interest to review your lender's instructions and those from any other partners very carefully. This will help you understand steps you may be asked to take regarding the handling of the consumer's private information, specifically regarding how it may be used, retention limits, and redaction or deletion requirements.

What to Do Next

As you plan for your strategy and ability to thrive in the new privacy-focused title and settlement services landscape, consider the following:

1. **Are you in compliance with the Gramm-Leach-Bliley Act and any state-specific privacy requirements that are currently in place?** Review your current privacy policy that explains your policies and practices regarding consumer's private information.
2. **Are you a business subject to the CCPA?** Remember the law's three-part test:
    a. Doing business with California residents (whether you are in California or not),
    b. Collecting the personal information of these consumers and
    c. Being a for-profit entity that has at least $25 million in annual gross revenues or collects, buys, shares, or sells at least 50,000 consumers' personal information annually, including any controlling or controlled entities that share common branding with you.

If the answer is yes to the above, review the checklist below that outlines the minimal steps you need to take to comply with CCPA and any applicable timelines. Remember that CCPA covers more categories of information than the GLBA, and the private right-of-action in CCPA in case of data breaches also applies to information categories covered by the GLBA. Even if you are not a business under the CCPA, consider whether you're a service provider or a third party under the CCPA and examine the requirements applicable to those entities.

3. If you are currently exempt from CCPA but will meet the requirements of the test outlined above soon, plan and implement the same checklist.
4. If you are subject to other newly enacted state privacy laws or expect one to become law soon, compare those requirements to your processes and practices regarding CCPA and plan to accommodate any new requirements.

Minimal Action Item Checklist

1. Update your privacy policy in consultation with your legal counsel, and implement any required notices on your website and communications. You should do this as soon as practicable.
2. Implement one set of consistent policies and procedures, matching the most stringent requirements you are presented with to reduce your operational complexity. Have the broad outline of your process in place as of January 1, 2020, with the details resolved by the end of January 2020.
3. Implement the required mechanisms to receive requests, to verify them, and to deliver the outcome of the request or the reasons for the denial. This should be in place, even as a draft, as of January 1, 2020.

4. Ensure staff is trained to receive and respond to a consumer's request, how to verify it, where to store it, and how to deliver the outcome of the analysis to the requestor. Ideally, have a single intake point for all requests rather than having each team respond individually. Advise your staff of the compliance requirements as soon as possible, and designate a single point of contact as of January 1, 2020.
5. Design and implement a streamlined workflow for verifying the request and the requestor, obtaining the information requested, having it reviewed by appropriately qualified resources, and delivering it to the consumer in a secure way. CCPA explicitly requires the authentication of the identity of the requestor for the request to be verifiable. If you have a previously verified account for the consumer, that is an acceptable method.

Note: You will have to implement another verification method for consumers who may not have a previously verified relationship with you. CCPA states explicitly that the creation of an account with your business as part of the verification process may not be the sole method, and only allows a business to request additional information to verify the requestor's identity if the identity cannot be verified from maintained information. The (currently) draft regulations implementing CCPA state that non-public information collection is allowable to verify a request.

6. Ensure your verification workflow and retention method of this request is in place by February 1, 2020. Recall that you have 45 days to respond to a verifiable request, although you may request an extension of up to 45 days, should the circumstances require it. However, you need to deliver the reasons for the extension to the consumer within the first 45 days.
7. Consult with your legal counsel regarding a deletion request. Recall that your responsibilities under the CCPA can be preempted by other legal obligations, such as maintaining records of a settlement transaction for a number of years. Also, there are multiple exemptions in the law that might be applicable, such as the need to complete an ongoing transaction.
8. Being able to track consumer's opt-out, information, and deletion requests correctly will be key to demonstrate compliance. Ensure that you have the necessary system in place by February 1, 2020.
9. Engage your institutional customers of scale (e.g., lenders, secondary market participants, builders) and understand how they plan to design and implement procedures for compliance. Work towards a streamlined solution that accommodates your compliance needs and operational efficiency.
10. If you've already received any partner-driven requests for data discovery, redaction, or deletion, be sure to follow up with your partner to understand and memorialize their expectations. If necessary, create processes to track and comply.
11. Ensure that your information security policies and practices are up to date and enforced.
12. Enlist help from your title and settlement software provider regarding how data is stored in your system of record, what is transmitted to or received from third parties, and how it is processed. If you are a ResWare user, please consult the section below about how ResWare can help you comply with CCPA and other similar legislation.

13. Review and, if necessary, amend your service provider agreements to comply with the CCPA and include permissible uses of consumer data that you are sharing with them and especially to understand if they can or do sell the data you provide to them. If you do receive a valid deletion request, engage all your service providers with whom this consumer's information was shared and cause them to delete any relevant records as well. Be sure to include this requirement in your agreements. Aim to finalize the amendments by the end of March 2020.
14. Keep abreast of any new developments in the privacy sphere in the states in which you operate.

As mentioned, a new and updated California's Privacy Rights Act (CPRA) has been submitted as a citizen's initiative in California, which will aim to also introduce transparency into the use of automated decision making and new limitations on the use of personal information. Review the American Land Title Association's (ALTA) data privacy website. In addition to ALTA, your business partners, state land title associations, and underwriters are good resources.

How ResWare Helps You Be Efficient and Compliant

ResWare, as your system of record for your title and settlement business, contains a great amount of information that is subject to the privacy-focused laws explained in this whitepaper. Our goal is not to just help you comply, but also retain the efficiency afforded to you by ResWare while you remain compliant. To that end, the following resources are available for your adoption. Materials for ResWare customers are available on the ResWare customer portal or through our support channels by the dates listed below.

1. ResWare architecture diagram and documentation, including configuration changes, for a more secure ResWare deployment: available on the customer portal
2. ResWare data storage and classification documentation to help identify the categories and locations of information stored in ResWare: available on the customer portal.
3. Use the database scripts as a sample to add links to your privacy policy and "Do not sell my info" opt-out pages: available on the customer portal
4. Data mapping for ResWare's integration endpoints, identifying what data are sent and received on each integration request and their classification: available in this matrix
5. Guidance and tooling to discover what personal information is stored in ResWare about a consumer: estimated availability June 30, 2020.
6. Guidance and tooling to delete (where possible) consumer's personal information: estimated availability is June 30, 2020.
7. Additional work has been done to review and remove unneeded information from ResWare's log streams, to help reduce your data mapping surface. **If you are on a version of ResWare prior to 9.7.58, 9.8.29, or 9.9.11, you will need to upgrade ResWare to receive these changes.** Please contact support@adeptive.com to request an upgrade.

GLBA Data Points

Thanks to the GLBA exemption for data collected during the provision of a financial service of a product, many data points that might have normally been subject to the CCPA are exempt, but other iterations of the CCPA or other states' versions of consumer privacy laws may have different requirements and exemptions. However, do remember that the private right of action of a consumer due to a data breach extends to the data points covered by the GLBA. Hence, it's very important that you review your information security practices and encrypt your transactional data and documents at rest and in transit when possible.

As we navigate the rapidly changing privacy landscape together, we are committed to providing you with the resources you need to remain at the forefront of efficiency while remaining compliant.

Please contact support@adeptive.com with any inquiries, comments, or feedback regarding this privacy whitepaper. This whitepaper is intended to contain general advice and information that we hope you will find useful but is not a substitute for the advice of your legal counsel. It is provided to you at no charge on an as-is, best-effort basis, and conveys no warranty or guarantee of performance of any kind.

Acknowledgments

We gratefully acknowledge the invaluable insights, comments, and contributions of our partners to this white paper.