A Simple Approach to Complying with Privacy Regulation

States have been enacting their own privacy regulations, creating a patchwork system of regulation.[1] The style and topic of the regulations varies across states and the variations in the regulation create compliance challenges for businesses.[2] This piece will illustrate the compliance challenges the patchwork system of privacy regulation creates and propose that businesses could treat the patchwork system as a single privacy regulation. Under this approach, businesses would create their own privacy compliance system by taking the strictest requirements from each privacy regulation, essentially treating them as a single privacy regulation. This approach would remove the state boundaries to the patchwork system and simplify privacy compliance.

For illustrative purposes, suppose a business is a financial institution that furnishes health savings accounts on behalf of a health plan and has consumers in California, Colorado, and Utah. Because the business is a financial institution, it will be subject to the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulation, Regulation P ("Reg P").[3] California also has its own financial information privacy act, namely, the California Financial Information Privacy Act ("CalFIPA").[4] Under the GLBA, states may implement regulations that are stricter than the GLBA.[5] So, when the requirements of CalFIPA are stricter than the standards of the GLBA and Reg P, the financial institution will need to comply with CalFIPA.

[1] *E.g.*, CAL. CIV. CODE § 1798.100-1798.199.100; COLO. REV. STAT. § 6-1-1301 et seq.; DEL. CODE ANN. tit. 6, §12D; IND. CODE § 24-15; IOWA CODE § 715D; TEX. BUS. & COM. CODE ANN. § 541 (West); UTAH CODE ANN. § 13-61-101 et seq.; VA. CODE ANN. § 59.1-575 et. seq.
[2] *Compare* CAL. CIV. CODE § 1798.100-1798.199.100 *with* COLO. REV. STAT. § 6-1-1301 et seq.
[3] 15 U.S.C. § 6821 et seq.; 12 C.F.R. 1016.1-17.
[4] CAL. FIN. CODE § 4050-60.
[5] Financial Services Modernization (Gramm-Leach-Bliley) Act, Pub. L. No. 106-102, 113 Stat. 1338, 1436-37 (codified as amended at 15 U.S.C. § 6824).

Additionally, California, Colorado, and Utah each have separately enacted similar but distinct privacy regulation.[6] Assume the business meets the applicability threshold for the California Consumer Privacy Act ("CCPA"), Colorado Privacy Act ("CPA"), and Utah Consumer Privacy Act ("UCPA").[7] Under the regulations' exemptions, the CCPA will apply but the CPA and UCPA will not.[8] The variation in language across the three Acts is worth noting.

Just examining the varying rights that consumers receive under the CCPA, CPA, and UCPA will highlight the patchwork regulatory system created by state privacy acts. Under the CCPA and CPA but not the UCPA, consumers have a right to correct their information.[9] The CPA includes a right to opt in for processing of sensitive personal information.[10] Under the CCPA, consumers can opt out of automated decision making that utilizes sensitive personal information.[11] The UCPA does not consider a similar right but it provides a right to opt out of automated decision making for the purposes of targeting the consumer for advertising.[12] The CPA contains this opt out right but the CCPA does not.[13] As highlighted by these variations, businesses that are subject to numerous state privacy regulations are subject to a patchwork of requirements.

The CCPA exempts "personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act…".[14] The subject of this exemption is "personal information" rather than the business. Accordingly, information a financial institution utilizes that

[6] CAL. CIV. CODE § 1798.100-1798.199.100; COLO. REV. STAT. § 6-1-1301 et seq.; UTAH CODE ANN. § 13-61-101 et seq.
[7] UTAH CODE ANN. § 13-61-101 et seq.
[8] CAL. CIV. CODE § 1798.145(e); COLO. REV. STAT. § 6-1-1304(2)(q); UTAH CODE ANN. § 13-61-102(2)(k).
[9] CAL. CIV. CODE § 1798.106; COLO. REV. STAT. § 6-1-1306(c); *see generally* UTAH CODE ANN. § 13-61-101 et seq.
[10] COLO. REV. STAT. § 6-1-1308(7).
[11] CAL. CIV. CODE § 1798.121(b).
[12] UTAH CODE ANN. § 13-61-201(4)(a).
[13] COLO. REV. STAT. § 6-1-1306(a)(I)(C).
[14] CAL. CIV. CODE § 1798.145(e).

falls outside of the scope of the GLBA, its implementing regulations, or CalFIPA, will not be exempt from the CCPA. A likely example of such information is website cookies.[15]

The CPA excepts "A financial institution or an affiliate of a financial institution as defined by and that is subject to the Federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq., as amended, and implementing regulations, including Regulation P, 12 CFR 1016."[16] This clearly excepts all financial institutions, including the hypothetical financial institution.

The UCPA contains language similar to the CPA.[17] But the UCPA's language is less clear. The UCPA states that it does not apply to "a financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., and related regulations."[18] There are two ways to read this language.

---

[15] But note that this example may be debatable. Reg P prohibits financial institutions from disclosing nonpublic personal information to nonaffiliated third parties unless the financial institution provides a proper disclosure or the financial institution shares the information for its ordinary business as a financial institution. 12 C.F.R. §§ 1016.10, 1016.14. But the definition of "nonpublic personal information" has limited scope. *See* 12 C.F.R. § 1016.3(p). The term is defined, through the incorporation of the definition of "personally identifiable financial information," as any information a consumer provides to the financial institution in connection with providing a financial product or service to that consumer. 12 C.F.R. §§ 1016.3(p)(1)(i), 1016.13(q). Whether a consumer provides website cookies to a financial institution in connection to a financial product or service is unclear. Certainly, financial institutions have websites for the purpose of providing financial products and services. However, a person does not need to visit a financial institution's website in connection to a financial product or service. For example, a person could visit a financial institution's website to gather ideas on how to design her own website and provide the financial institution information through website cookies. Notice, Reg P contemplates the reason that the consumer provided information to the bank. *See* 12 C.F.R. § 1016.3(q) (defining personally identifiable financial information as information that "[a] consumer provides to you to obtain a financial product or service," "resulting from any transaction involving a financial product or service" or the financial institution "obtain[s] about a consumer in connection with providing a financial product or service to that consumer"). In this example, the person does not visit the financial institution's website in connection to a financial product or service. So, information the financial institution gathered from website cookies would not be "nonpublic personal information" and, therefore, not subject to the GLBA or its implementing regulation. This example is debatable because a regulator could still argue that the person visited the website in connection to a financial product or service. After all, the website exists because of financial products or services. So, any visit to the financial institution's website might be connected to a financial product or service.

[16] COLO. REV. STAT. § 6-1-1304(2)(q).

[17] *Compare* UTAH CODE ANN. § 13-61-102(2)(k) *with* COLO. REV. STAT. § 6-1-1304(2)(q).

[18] UTAH CODE ANN. § 13-61-102(2)(k).

The two readings are made apparent by contrasting the language of the UCPA with the language of the CPA. Unlike the CPA which excepts financial institutions "subject to" the GLBA as a whole, the UCPA does not apply to financial institutions that are "governed by" the privacy specific chapter of the GLBA. The GLBA amended what are considered financial activities under the Bank Holding Company Act of 1956.[19] Therefore, the GLBA will generally apply to any financial institution, but whether a particular section applies in a particular circumstance is less clear. So, the CPA's language is easy to understand because it does not leave a question about when a particular section of the GLBA may apply to a financial institution. In contrast to the CPA, the UCPA's "governed by" language could be read generally or as applying to specific situations. When reading the UCPA to not apply to a financial institution that is *generally* "governed by" Title V of the GLBA, the UCPA will not apply to any financial institution in any circumstance. However, if the UCPA's "governed by" language is read to only exclude financial institutions in the specific circumstances under which Title VII of the GLBA applies, then the UCPA could apply in other circumstances, such as when a financial institution collects information through website cookies. Thus, whether "governed by" has general or specific applicability determines whether the UCPA applies.

The UCPA's language that exempts financial institutions could have specific applicability, though that is unlikely for a few reasons. If "governed by" has specific applicability, then the entire clause "a financial institution or an affiliate of a financial institution governed by" is redundant with subsequent clause "personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act." That is, under the specific applicability reading, a financial institution is only "governed by" Title VII of the GLBA when it collects, processes, sells,

[19] Financial Services Modernization (Gramm-Leach-Bliley) Act, Pub. L. No. 106-102, 113 Stat. 1338, 1342-51.

or discloses personal data in accordance with Title VII of the GLBA. Therefore, the better reading is that "governed by" has general applicability and that financial institutions are always exempt from the UCPA.[20]

Turning back to the previous hypothetical, as discussed, the GLBA, its implementing regulations in Reg P, CalFIPA, and the CCPA apply to the financial institution. Recall, the financial institution is furnishing health savings account on behalf of a health plan. Accordingly, the Health Insurance Portability and Accountability Act ("HIPAA") is a regulation that could apply to the financial institution.[21] But under HIPAA, the business will be a "business associate" to the health plan which is a "covered entity".[22] This means the financial institution is not the primary concern of HIPAA but the covered entity is required, by HIPAA, to impose confidentiality and reporting requirements on the financial institution through its agreement with the financial institution.[23]

Next, consider the requirements that the applicable regulations impose on a financial institution. For simplicity, this discussion will only consider the initial notice requirements imposed by the regulations. This includes, for example, what the regulations require the hypothetical financial institution to inform consumers of at the beginning of their interactions with the consumer. Under HIPAA, because the financial institution is not a covered entity, it does not have any initial notice requirements.[24] And thus, the financial institution's regulatory compliance only includes the GLBA, as implemented by Reg P, CalFIPA, and the CCPA.

---

[20] There is a counterargument to this understanding. When comparing the language of the UCPA to the CCPA, the two appear similar. They both exempt information collected, processed, sold, or disclosed in accordance with the GLBA. Arguably, the UCPA's clause "a financial institution or an affiliate of a financial institution governed by" is merely adding a signal to financial institutions that this is where they can find their exemption.
[21] *See* 45 C.F.R. § 160.102.
[22] 45 C.F.R. § 160.103.
[23] *See generally* 45 C.F.R. §§ 160.102, 160.103, and 160.310.
[24] 45 C.F.R. § 164.520(a)(1).

Through its privacy notice, Reg P requires that financial institutions disclose the categories of nonpublic personal information that it collects and discloses, the categories of affiliates and nonaffiliated third parties to whom the financial institution discloses information, and information related to the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties.[25] Note, Reg P's opt out right is limited to opting out of disclosure of nonpublic personal information to a nonaffiliated third-party, except when the financial institution has contracted the nonaffiliated third-party to provide financial products and services.[26] Significantly, CalFIPA expands this opt out right to also include opting out of the disclosure of personal and financial information to affiliated third parties and removes the contracted third-party exception from nonaffiliated third-party opt outs.[27] However, CalFIPA excepts the disclosure of "nonpublic personal information [that] is necessary to effect, administer, or enforce a transaction requested or authorized by the consumer…".[28] Accordingly, because of this exception, the notice requirements of CalFIPA collapse into the notice requirements of Reg P and CalFIPA does not impose requirements that are additional to Reg P.

The CCPA, however, increases a financial institution's initial notice requirements. Similar to Reg P, the CCPA requires the disclosure of categories of personal information collected by a business and the purposes for which it collected, including selling the information.[29] Additionally, businesses must disclose the consumer's right to delete personal information, right to correct inaccurate personal information, right to access personal information, right to know what personal

[25] *See* 12 C.F.R. § 1016.6.
[26] 12 C.F.R. § 1016.10(a)(2).
[27] CAL. FIN. CODE § 4053.
[28] CAL. FIN. CODE § 4056.
[29] CAL. CIV. CODE § 1798.100.

information is sold or shared and with whom, and right to opt out of the sale or sharing of personal information.[30]

A financial institution has two options for complying with the Reg P and CCPA requirements. One option is to treat the two separately with separate disclosures and to provide all consumers a Reg P disclosure while limiting the CCPA disclosure to California consumers. The other option is to provide all consumers, regardless of residency, a single disclosure that complies with the requirements of Reg P and the CCPA. This approach has advantages in simplicity. The financial institution will not need to process disclosures or requests based on the consumer's residency. But the approach has a disadvantage in affording rights to consumers that the current regulatory landscape does not give those consumers.

As states continue to enact their own privacy regulations, the complexity of the patchwork of regulatory requirements increases. Recall the patchwork of requirements that exist between the CCPA, CPA, and UCPA. Complying with each of these on a state-by-state basis would require a business to maintain separate policies on how to treat a consumer's information and privacy requests based on his or her residency. A simpler option is to merge the requirements and to comply with the strictest requirements across jurisdictions. This immunizes a business from state-by-state changes to the regulatory landscape that do not affect the strictest requirements, while demonstrating a respect for consumers' privacy rights, regardless of where the consumer resides. This approach also allows businesses to operate simply, as though there is a single privacy regulation with which it must comply.

[30] CAL. CIV. CODE § 1798.105-120. CAL. CIV. CODE § 1798.121 also includes a notice requirement for a consumer's right to limit the use and disclosure of sensitive personal information. I ignore this section for simplicity.